TRAITE DE)OPERATION EN MATIERE ~ BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 26 juin 2000 (26.06.00)	
Demande internationale no PCT/FR99/02678	**Référence du dossier du déposant ou du mandataire** GEM 555
Date du dépôt international (jour/mois/année) 03 novembre 1999 (03.11.99)	**Date de priorité** (jour/mois/année) 13 novembre 1998 (13.11.98)
Déposant BIRKNER, Marc etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

25 mai 2000 (25.05.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Christelle Croci

no de téléphone: (41-22) 338.83.38

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G06K 19/073, G07F 7/10

A1

(11) Numéro de publication internationale: **WO 00/30030**

(43) Date de publication internationale: 25 mai 2000 (25.05.00)

(21) Numéro de la demande internationale: PCT/FR99/02678

(22) Date de dépôt international: 3 novembre 1999 (03.11.99)

(30) Données relatives à la priorité:
98/14517 13 novembre 1998 (13.11.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: BIRKNER, Marc [FR/FR]; 2 Résidence Saint Joseph, F–13950 Cadolive (FR). GIRAUD, Jean, Luc [FR/FR]; 22, rue du Four, F–13400 Aubagne (FR). TALVARD, Laurent [FR/CA]; 425, rue de la Noue, Verdun, Ile des Soeurs, QC H3E 1R9 (CA).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

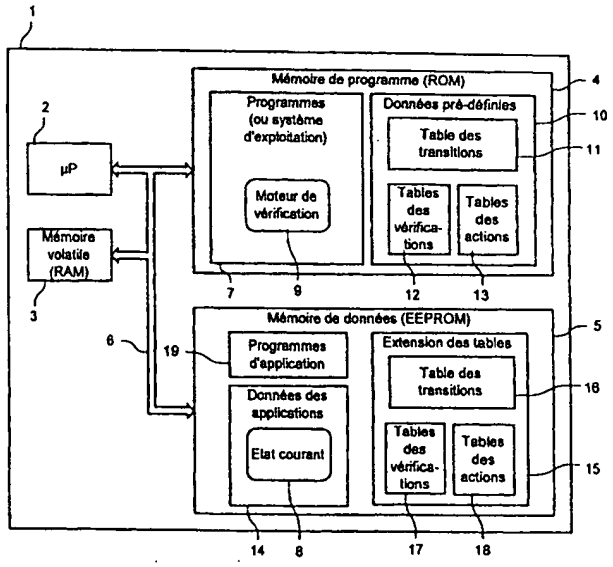
Avec rapport de recherche internationale.

(54) Title: METHOD AND DEVICE FOR CONTROLLING A PORTABLE OBJECT LIFE CYCLE, IN PARTICULAR A SMART CARD

(54) Titre: PROCEDE ET DISPOSITIF DE CONTROLE DU CYCLE DE VIE D'UN OBJET PORTATIF, NOTAMMENT D'UNE CARTE A PUCE

(57) Abstract

The invention concerns a device and a method for controlling a portable object life cycle, in particular a smart card (1), the life cycle being determined by successive of state transitions, said states determining the services offered by the object, said object comprising a processing unit (2), programme storage units (4) and data storage units (5), each of said storage unit having a content defining a plurality of configurations. The device is characterised in that it comprises means controlling (9, 11, 12) the transition from one first state to a second state of said object and, preferably means for triggering actions when the transition crossover from one state to another occurs or when such a transition crossover request is denied. The method is characterised in that it comprises a plurality of steps dependent on the type of transitions implied in the request for state transition crossover applied to the object.



2... MICROPROCESSOR
3... VOLATILE MEMORY (RAM)
4... PROGRAMME MEMORY (ROM)
7... PROGRAMMES (OR OPERATING SYSTEMS)
9... VERIFICATION DRIVE
10... PRE-DEFINED DATA
11,16... TRANSITION TABLE
12,17... VERIFICATION TABLE
13,18... ACTION TABLE
5... DATA STORAGE (EEPROM)
19... APPLICATION PROGRAMMES
14... APPLICATION DATA
8... CURRENT STATE
15... TABLE EXTENSION

(57) Abrégé

L'invention concerne un dispositif et un procédé de contrôle du cycle de vie d'un objet électronique portatif, notamment une carte à puce (1), le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires présentant un contenu définissant une pluralité de configurations. Le dispositif est caractérisé en ce qu'il comprend des moyens de contrôle (9, 11, 12) de la transition d'un premier état à un second état dudit objet et, préférentiellement des moyens permettant de déclencher des actions lors du franchissement ou du rejet du franchissement de la transition d'état demandée. Le procédé est caractérisé en ce qu'il comprend une pluralité d'étapes dépendantes du type des états impliqués dans la demande de franchissement de transition d'état appliquée à l'objet.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE ET DISPOSITIF DE CONTROLE DU CYCLE DE VIE D'UN OBJET PORTATIF, NOTAMMENT D'UNE CARTE A PUCE

L'invention concerne les objets électroniques portatifs tels que les cartes à microcircuits électroniques, dites cartes à puce qui, connectées à des dispositifs électroniques pour permettre à ces derniers de réaliser des fonctions particulières dans le cadre d'une ou plusieurs applications, nécessitent un contrôle de leurs étapes de vie. Lesdites cartes sont en effet généralement utilisées dans des applications (banque, communication, identité, santé...) nécessitant une grande sécurité contre les usages frauduleux. L'invention s'applique plus généralement à tout système embarqué indépendant, doté d'une unité de traitement et des mémoires de programme et de données.

Il est connu dans le monde de la carte à puce que celle-ci résulte d'un assemblage d'un composant (comprenant en général un microprocesseur en relation avec des mémoires via des bus de communication), d'un module (réalisé à l'aide d'un métal conducteur) auquel est relié ledit composant (dans le cadre d'une carte à puce dite à contact) pour permettre audit composant d'être connecté à un dispositif électronique de lecture et/ou écriture (ou coupleur) et d'un corps de carte ou plus généralement d'un support sur lequel est intégré l'ensemble module/composant. Dans la cadre d'une carte à puce dite sans contact, ledit module est remplacé par une antenne et l'ensemble formé par le composant et ladite antenne est intégré au sein dudit support.

La vie d'une carte à puce se décompose généralement en deux ensembles d'étapes se succédant les unes aux autres, correspondant respectivement à la fabrication et à l'exploitation de ladite carte. La composition des deux ensembles d'étapes forme un cycle de vie de ladite carte.

La fabrication d'une carte à puce (à contact ou sans contact) est constituée de plusieurs étapes.

En effet, il est tout d'abord nécessaire de disposer d'un composant électronique qui est initialisé, isolé, puis relié à un module. Ledit composant et le module, auquel il est relié, sont par la suite intégrés sur ou au sein d'un support (généralement un corps de carte plastique) lui même imprimé à des fins d'identification ou de publicité. Par la suite la carte à puce ainsi obtenue est initialisée ou programmée pour répondre aux conditions d'utilisation dans le cadre d'applications.

Le second ensemble d'étapes de vie d'une carte à puce correspond à son exploitation. Cet ensemble peut lui-même être divisé en plusieurs étapes, chacune correspondant, par exemple, à l'implantation ou la suppression de services offerts par la carte à puce à l'utilisateur en fonction de son profil par exemple.

En outre différents acteurs (fabricant de composant, fabricant de cartes à puce, centre de personnalisation de cartes, émetteur de cartes, ou encore porteur de cartes) interviennent durant les différentes étapes de la fabrication et de l'exploitation d'une carte à puce. Ainsi, les composants sont fournis et parfois en partie initialisés par des fabricants de composants électroniques sur une tranche de silicium. Cette phase correspond à l'étape de fabrication du composant. L'étape suivante est la phase d'encartage réalisée par le fabricant de carte à puce. Elle inclut l'isolement d'un composant de la tranche de silicium, la connexion dudit composant à un module (ou antenne), l'intégration de l'ensemble sur leur support ou corps de carte. Suit la préparation de la structure applicative présente dans la mémoire programmable électriquement du composant. C'est l'étape de personnalisation électrique qui est réalisée par le fabricant des cartes à puce ou par un centre de

personnalisation ou un tiers spécialisé dans la personnalisation des cartes ou par l'émetteur lui-même qui est chargé in fine de la distribution des cartes sur le marché. Cette phase de personnalisation électrique peut donc être décomposée en autant d'étapes qu'il y a acteurs ou d'intermédiaires. Par la suite, durant l'exploitation de la carte à puce, nous avons vu précédemment qu'il peut être intéressant de distinguer différentes étapes au gré de l'évolution du profil de l'utilisateur de la carte par exemple.

Quoi qu'il en soit, il est donc important de suivre rigoureusement les étapes de vie d'une carte pour connaître à tout moment l'étape en-cours de ladite carte au sein de son cycle de vie. De plus, il est indispensable que, d'une part, l'accès en écriture ou en lecture de la mémoire programmable électriquement du composant d'une carte soit protégé durant l'échange de ladite carte (ou du composant) entre les différents acteurs et que d'autre part l'accès à ladite mémoire soit limité au fur et à mesure que se succèdent les étapes de vie de la carte citées précédemment, en activant ou désactivant des services par exemple. Pour finir, il est également nécessaire parfois de valider le contexte applicatif de la carte à puce avant que le porteur de celle-ci l'utilise sur le marché. Par exemple, un émetteur de carte à puce de type porte-monnaie électronique, doit être certain que la balance de ladite carte est bien nulle avant d'émettre la carte.

Pour tenter de répondre à ces exigences, différentes solutions sont utilisées à ce jour. Certaines solutions sont purement extérieures à la carte à puce (sécurisation physique des locaux où ladite carte est fabriquée, utilisation de moyens de transport eux-mêmes sécurisés...). D'autres solutions complémentaires aux premières, mais cette fois internes ou implantées dans la carte, sont aussi

généralement utilisées. On utilise ainsi des secrets permettant de protéger l'accès en lecture/écriture de la mémoire du composant et également des indicateurs logiques permettant de suivre de manière irréversible les différentes étapes de vie de la carte. Pour cela, des bits au sein d'une mémoire non effaçable du composant de la carte à puce sont positionnés à l'état actif à la fin des différentes étapes de vie de la carte (fabrication et initialisation du composant par le fabricant dudit composant, encartage et initialisation de la mémoire de la carte par le fabricant de carte à puce, préparation de la structure applicative de la mémoire de la carte à puce par le centre de personnalisation ou l'émetteur de la carte...). En fonction de ces indicateurs, le programme (ou système d'exploitation), exécuté par le microprocesseur du composant de la carte à puce, implanté au sein de l'une des mémoires dudit composant de ladite carte, adapte son comportement au fur et à mesure que les étapes de vie de ladite carte se succèdent. Ainsi, des fonctions peuvent être modifiées, ajoutées ou supprimées.

Quelles que soient les solutions utilisées à ce jour, elles reposent toutes sur le fait que les différents acteurs impliqués dans la fabrication d'une carte sont des tiers de confiance. Seules des personnes, susceptibles d'intercepter des composants ou des cartes durant leur transfert entre deux des différents acteurs, sont supposées "fraudeurs potentiels" et les solutions exposées précédemment permettent de s'en affranchir. L'adaptation du système d'exploitation de la carte en fonction des indicateurs irréversibles apporte un plus non négligeable. Ainsi, si les fabricants de composants ou de cartes inscrivent des données systèmes ou des secrets, l'émetteur de la carte ne pourra par exemple librement s'affranchir desdits secrets ou modifier lesdites données système.

Cependant, cette solution ne résout pas le problème d'une initialisation frauduleuse de la carte ou d'une erreur malencontreuse durant ladite initialisation, effectuée par l'un des acteurs.

L'invention propose de remédier aux inconvénients de l'état actuel de la technique. En particulier, l'invention consiste à doter le système d'exploitation d'une carte à puce de moyens logiciels permettant audit système d'exploitation de maîtriser un changement irréversible d'étape de vie de ladite carte en fonction d'un ensemble de vérifications du contenu des mémoires de cette même carte à puce. En outre l'invention prévoit que lors d'un changement d'étape de vie, le système d'exploitation de la carte puisse déclencher automatiquement des actions permettant d'adapter les services offerts par ledit système d'exploitation de ladite carte.

A cet effet, l'invention concerne un dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant constitué par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, chacune de ces mémoires présentant un contenu définissant une pluralité de configurations, caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif.

Selon d'autres caractéristiques du dispositif selon l'invention :

- les moyens de contrôle comportent :
  - des moyens d'autorisation et/ou d'interdiction de transition d'états à effectuer;

- des moyens de vérification du contenu de la mémoire volatile, des mémoires de données et des mémoires de programme de l'objet électronique portatif en fonction de la transition d'états à effectuer;
- des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement d'une transition d'état.

En outre, l'invention concerne un objet électronique portatif, pouvant être notamment une carte à puce, comportant ledit dispositif de contrôle du cycle de vie.

Par ailleurs, l'invention concerne un procédé de contrôle du cycle de vie d'un objet électronique portatif, ledit procédé étant mis en œuvre au sein de l'objet à la suite d'une demande de transition d'états,

caractérisé en qu'il comprend :

- une étape de validation de l'autorisation de ladite demande;
- une étape d'évaluation des vérifications associée à la transition demandée;
- une étape de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée et, si les vérifications de la configuration de l'objet sont satisfaites.

Selon d'autres caractéristiques, le procédé comprend éventuellement en outre :

- une étape d'exécution d'actions systématiques;
- une étape d'exécution d'actions positives dans le cas où la transition demandée est autorisée et si les vérifications associées à la transition demandée sont satisfaites;

- une étape d'exécution d'actions négatives dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre indicatif et nullement limitatif de l'invention.

Les figures montrent:

- figure 1: un composant d'une carte à puce munie d'un dispositif de vérification de transition d'état;
- figures 2a et 2b: une représentation détaillée d'une table des transitions d'état;
- figure 3: une représentation détaillée d'une table des vérifications des transitions;
- figure 4: une représentation détaillée d'une table des actions;
- figure 5: une description des étapes mises en ouvre dans le procédé utilisé par le dispositif de vérification de transitions;
- figures 6a à 6d: les particularités mises en œuvre dans le cas d'un exemple d'une carte à puce de type porte-monnaie électronique.

Dans l'invention, on appellera état de référence, un état à partir duquel il est possible de basculer vers un autre état suite au franchissement d'une transition décrite dans la table des transitions, implantée dans la mémoire de programme. Comme il est décrit plus loin, il est possible d'ajouter de nouveaux états et donc de nouvelles transitions après que l'étape de fabrication du composant ait eu lieu. Dans ce cas, on parlera d'états additifs pour caractériser ceux-ci par opposition aux états de référence. D'autre part, on appellera état courant l'état dans lequel se trouve le système embarqué.

La figure 1 montre un composant 1, d'une carte à puce, muni d'un dispositif de vérification de transitions selon l'invention. Le composant comporte une unité de traitement 2 ou encore microprocesseur en relation avec des mémoires 3, 4 et 5 via un bus de communication 6. Une mémoire de programme 4 (ou encore ROM) non effaçable comporte d'une part une zone de programmes 7, lesdits programmes (ou encore système d'exploitation du système embarqué) pouvant être exécutés par ladite unité de traitement et d'autre part une zone de données prédéfinies 10 qui contient des constantes utilisées par ledit système d'exploitation. Parmi lesdites constantes de la zone 10, le système d'exploitation 7, comportant un programme appelé moteur de vérification 9, exploite une table des transitions 11 qui permet de préciser les états auxquels on peut accéder à partir de l'état courant, une table des vérifications 12 qui permet d'associer à chaque transition d'état des vérifications portant sur le contenu des mémoires 3, 4 et/ou 5. Dans une variante, le moteur de vérification 9 peut déclencher automatiquement des actions lors du franchissement ou du rejet du franchissement d'une transition. Pour cela la zone 10 de la mémoire de programme comporte une table des actions 13 qui permet d'associer à chaque transition d'état possible des actions à effectuer.

Une mémoire volatile 3 (ou encore RAM pour Random Access Memory en langue anglaise) permet à l'unité de traitement 2 de stocker de manière temporaire des résultats ou encore des secrets issus de calculs décrits par les programmes implantés dans la mémoire de programme 4. Le contenu de la mémoire 3 est effacé à chaque mise sous tension du composant 1 ou à chaque demande de remise à zéro de celui-ci.

Une mémoire de données 5, effaçable électriquement utilisant généralement la technologie EEPROM (pour

Electrical Erasable Programmable Read Only Memory en langue anglaise) comporte une zone 14 contenant les données variables nécessaires à l'exécution des programmes 7. Cette zone 14 comporte notamment une donnée 8 appelée "Etat courant" permettant de mémoriser l'état courant de l'objet électronique portatif. La mémoire de données 5 comporte en outre une zone 15 comprenant optionnellement des extensions des tables 11 à 13 dans le cas où il est nécessaire d'ajouter des états aux états de références. La zone 15 comporte alors une extension de la table des transitions 16, une extension de la table des vérifications 17 et peut comporter une extension de la table des actions 18 si l'on souhaite associer aux nouvelles transitons d'état additif des actions, comme vu précédemment pour ce qui concerne la table 13. Dans le cas d'ajout d'états par rapport aux états de référence, il est parfois indispensable d'enrichir le système d'exploitation 7. Pour cela, la mémoire 5 peut comporter en outre une zone 19 qui contient les programmes supplémentaires qui seront exécutés à leur tour par l'unité de traitement 2.

La figure 2a montre une mise en ouvre possible de la table des transitions 11. Si l'on suppose que l'on dénombre i états de référence, on peut imaginer une table de transition comprenant i colonnes et i lignes. Les colonnes correspondent aux états de référence pouvant être, à un instant donné, l'état courant. Les i premières lignes correspondent aux états de référence auxquels on peut accéder à partir de l'état courant. Ainsi la valeur d'une case de la table des transitions 11 correspondant à l'intersection d'une ligne et d'une colonne de ladite table permet de coder soit, l'absence de transition autorisée (valeur nulle par exemple - c'est le cas de la transition 20), soit, l'autorisation une transition (valeur non nulle - c'est le cas de la transition 21). Dans le cas d'une

transition autorisée, le moteur de vérification de transitions recherche au sein de la table de vérification 12 les vérifications à effectuer pour accepter ou rejeter le franchissement de la transition demandée.

La figure 2b montre également une mise en ouvre possible d'une table de transition dans le cas où il est possible d'ajouter des états (états additifs) aux états de référence. La table des transitions comporte une ligne supplémentaire par rapport à la figure 2a. La (i+1)ème ligne permet de préciser si l'on autorise des transitions d'un état de référence courant à un état additif. Ainsi la valeur de la case 22 indique une transition interdite d'un état de référence vers un état additif. La case 23 indique qu'il sera possible de basculer de l'état de référence Ei vers un état additif. Une extension 16 de la table des transitions est alors nécessaire. Cette dernière comporte j lignes correspondant à j états additifs auxquels on peut accéder à partir de (i+j) états courant possibles matérialisés par les (i+j) colonnes de l'extension 16 de la table des transitions. Ainsi la combinaison de la case 23 de la table des transitions et de la case 24 de l'extension 16 de la table des transitions, indique au moteur de vérification qu'il est possible de basculer de l'état de référence Ei vers l'état additif E(i+1).

La figure 3 montre une mise en ouvre de la table des vérifications. La table des vérifications 12 est implantée au sein de la zone 10 des données prédéfinies de la mémoire 4. Chaque transition autorisée dispose d'une entrée dans ladite table. Une entrée comprend un champ 30 permettant d'identifier la transition et un champ 31 contenant une référence (ou adresse) vers un programme 32 du système d'exploitation 7. Le moteur de vérification 9 peut ainsi faire exécuter à l'unité de traitement 2 les contrôles

requis pour accepter le franchissement de la transition. La figure 3 illustre également une structure d'une extension 17 de la table des vérifications. De la même manière que pour la table 12, l'extension de la table des vérifications 17 comporte une entrée par transition possible. Chaque entrée comprend deux champs, un champ 33 permettant d'identifier la transition et un champ 34 contenant une référence (ou adresse) d'un programme 35 du système d'exploitation ou, comme le montre la figure 3, d'un programme supplémentaire implanté dans la mémoire de données 5 (en zone 19).

La figure 4 montre une représentation de la table des actions 13 implantée dans la zone 10 des données prédéfinies de la mémoire de programmes 4. Lors d'une demande de franchissement de transition, il est possible de déclencher des actions. Celles-ci peuvent être de trois types: action systématique, action positive (c'est à dire conditionnée au fait que les vérifications sont satisfaisantes) ou action négative (c'est à dire conditionnée au fait que les vérifications ne sont pas satisfaisantes). La figure 4 montre qu'à chaque transition autorisée, il existe une entrée dans la table des actions 13. Cette entrée comprend 4 champs. Le premier champ 400 permet d'identifier la transition. Les trois autres champs 401, 402 et 403 contiennent chacun une référence ou adresse d'un programme 404, 405 ou 406 du système d'exploitation. Le champ 401 est dédié à une action systématique, le champ 402 à une action positive et le champ 403 à une action négative. La figure 4 montre également une extension 18 de la table des actions. Cette table 18 est implantée dans la zone 15 de la mémoire de données 5 du composant 1. De la même manière que pour la table des actions 13, l'extension de la table des actions 18 comprend une entrée par transition possible. Une entrée comprend 4 champs. Le

premier champ 407 permet d'identifier la transition. Les trois autres champs 408, 409 et 410 contiennent chacun une référence ou adresse d'un programme 411, 412 ou 413 du système d'exploitation ou comme le montre la figure 4, des programmes implantés dans la zone 19 de la mémoire de données 5 du composant 1. Le champ 408 est dédié à une action systématique, le champ 409 à une action positive et le champ 410 à une action négative.

La figure 5a décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état de référence vers un autre état de référence. La demande de franchissement d'une transition peut être formulée suite à un ordre du fabricant de carte ou par tout autre acteur du cycle de vie de la carte à puce. Ladite demande peut également être formulée directement par la carte-elle même, par exemple au travers d'une action associée à une transition. Dans le cadre de la figure 5a, l'état de référence courant est l'état Ei. L'ordre 50 de basculement de l'état Ei à l'état Ej est formulé. L'étape 51 consiste à vérifier au sein de la table des transitions 11 que la transition de l'état Ei vers l'état Ej est autorisée. Dans le cas où cette transition est interdite, la demande de franchissement de transition 50 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela le moteur de vérification évalue l'entrée de la table des vérifications 12 dédiée à la transition T(Ei->Ej). L'exécution desdites vérifications correspond à l'étape 52 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de la table des actions 13 dédiées à ladite transition (étape 53). Si les vérifications 54 exigées lors de la demande de

franchissement de la transition 50 sont non satisfaisantes, l'état courant demeure inchangé. En fonction de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej) le moteur de vérifications exécute les actions négatives (étape 55 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 54 sont satisfaisante, alors l'état courant devient l'état Ej (étape 56 du procédé). Les actions positives sont alors exécutées (étape 57 du procédé) en fonction de l'état de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5b décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état additif vers un autre état additif. L'état additif courant est l'état Ei. L'ordre 510 de basculer de l'état additif Ei à l'état additif (ou de référence) Ej est formulé. L'étape 511 du procédé consiste à vérifier au sein de l'extension la table des transitions 16 que la transition de l'état Ei à l'état Ej est autorisée. Dans le cas où cette transition est interdite, la demande de franchissement de transition 510 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela, le moteur de vérification évalue l'entrée de l'extension de la table des vérifications 17 dédiée à la transition T(Ei->Ej). L'exécution desdites vérifications constitue l'étape 512 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de l'extension de la table des actions 18 dédiées à ladite transition (étape 513 du procédé). Si la vérification 514 exigée lors de la demande de franchissement de la transition 510 est non

satisfaisante, l'état courant demeure inchangé. En fonction de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej), le moteur de vérification 9 exécute les actions négatives (étape 515 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 514 sont satisfaisantes, l'état courant devient l'état Ej (étape 516 du procédé). Les actions positives sont alors exécutées (étape 517 du procédé) en fonction de l'état de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5c décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un état de référence vers un état additif. L'état de référence courant est l'état Ei. L'ordre 520 de basculement de l'état de référence Ei à l'état additif Ej est formulé. L'étape 528 du procédé consiste à vérifier au sein de la table des transitions 11, qu'une transition de l'état de référence courant Ei vers un état additif est autorisée. Si une telle transition est interdite, le procédé est terminé. L'état courant demeure inchangé. Par contre, si une transition dudit état de référence vers un état additif est autorisée, le moteur de vérification déroule les étapes 521 à 527 du procédé, respectivement identiques aux étapes 511 à 517 décrites en liaison avec la figure 5b.

Un exemple d'application dans le domaine du Porte-monnaie électronique est présenté en liaison avec les figures 6a à 6d. Ladite application permet de régler des achats à l'aide "d'argent électronique" stocké dans une carte à puce, au lieu de payer en numéraire. L'emploi d'une telle technique impose une gestion des cartes aussi sécurisée que celle qu'aurait imposé l'emploi du numéraire. Il faut par exemple éviter la création de monnaie fictive.

La sécurité d'une carte à puce porte-monnaie électronique repose généralement sur des clés stockées à l'intérieur de ladite carte à puce permettant des transactions sécurisées en utilisant la cryptographie. Une telle carte dispose d'un système d'exploitation offrant un jeu de commandes et de services permettant de créditer ou de débiter de l'argent. Au début du cycle de vie de la carte à puce porte-monnaie électronique, ladite carte à puce n'est pas initialisée. Elle ne contient aucune information. La figure 6a montre les états de référence prédéfinis :

- Etat E1 "carte vierge" (référencé 80): seules des commandes de test permettant de valider le comportement de la mémoire de données 5 sont disponibles (vérification que les cases mémoires de technologie EEPROM peuvent être correctement écrites et effacées);

- Etat E2 "carte testée" (référencé 82): Les commandes de test ne sont plus disponibles. A leur tour des commandes dites généralement "commandes physiques" (permettant un accès en écriture par un adressage physique indépendamment de toute structure logique de type fichier par exemple) sont disponibles. Elles permettent d'initialiser la carte (écriture dans la zone 14 de la mémoire de données des constituants logiques nécessaires au fonctionnement de l'application c'est à dire fichiers, balances...);

- Etat E3 "carte initialisée" (référencé 84): les commandes physiques ne sont plus disponibles. Des commandes logiques permettent de personnaliser la carte (ajout de nouvelles structures logiques et initialisation de données dans lesdites structures) sont utilisables. En outre, un mécanisme de recouvrement est activé de sorte que la carte à puce ne perde pas la cohérence de ces données lors d'une mise hors tension de celle-ci durant l'exécution de l'une desdites commandes logiques.

- Etat E4 "carte personnalisée" (référencé 86): les commandes logiques spécifiques à l'application Porte-monnaie électronique (débit/crédit) sont activées.

Le jeu de commandes disponibles évolue en fonction de l'étape de vie dans laquelle se trouve la carte à puce. Des informations stockées en mémoire de données permettent au système d'exploitation de connaître l'état dans lequel la carte à puce se trouve. La figure 6a montre en outre que dans le cadre d'une carte de type porte-monnaie électronique, toutes les transitions entre états de référence doivent être franchies successivement (de l'état E1 à l'état E4) et ce de manière irréversible. Toute autre transition est interdite. Seule la possibilité d'utiliser ultérieurement des états additifs 88 est offerte. Cette transition possible est référencée 87. Le système d'exploitation en fonction de l'état courant n'autorise qu'un ensemble de commandes spécifiques à chaque état de référence.

Les vérifications et les actions à déclencher lors du franchissement d'une transition sont décrites comme suit :

- Transition de l'état E1 vers l'état E2 (notée T(E1->E2) et référencée 81) :
  - Vérification: aucune
  - Action systématique :
    effacement de la mémoire de données pour éviter qu'un fraudeur y laisse des données interprétables par le système d'exploitation de la carte;
- Transition de l'état E2 vers l'état E3 (notée T(E2->E3) et référencée 83) :
  - Vérification:
    - intégrité des données écrites dans la mémoire de données avec les commandes physiques (validation d'un code de redondance par donnée);

- vérification de l'état vierge de la mémoire en dehors desdites données;
- Action positive :
  - activation du mécanisme de recouvrement;

- Transition de l'état E3 vers l'état E4 (notée T(E3->E4) et référencée 85) :
  - Vérification:
    - nullité de la balance du porte monnaie électronique
  - Action : aucune
- Transition de l'état E4 vers un état additif (notée T(E4->Eadd) et référencée 87) :
  - Vérification : aucune
  - Action : aucune

Les figures 6b à 6d illustrent respectivement une réalisation d'une table des transitions 11, d'une table des vérifications 12 et d'une table d'actions 13, selon l'invention. La table des transitions 11 telle que décrite en liaison avec la figure 6b permet de n'autoriser que les transitions 81, 83, 85 et 87. Pour cela seules les cases 60 à 63 de ladite table contiennent une valeur non nulle. Les autres cases de la table des transitions contiennent une valeur nulle pour indiquer que toute autre transition est interdite. La table des vérifications telle que présentée au travers de la figure 6c, permet d'associer les vérifications à satisfaire pour autoriser le franchissement des transitions 81, 83, 85 et 87, lesdites transitions autorisées par la table des transitions 11 (figure 6b). Ainsi l'entrée 64 de la table des vérifications 12 comporte un champ 641 permettant d'identifier que ladite entrée est dédiée à la transition 81. L'entrée 64 comporte en outre un champ 642 contenant une référence nulle pour indiquer qu'aucune vérification n'est demandée pour autoriser le franchissement de la transition 81. Dans une variante, la

transition 81 ne dispose d'aucune entrée associée. Cette variante est illustrée plus loin dans le cas de la table des actions. La table des vérifications 12 comporte une entrée 65 qui comprend respectivement un champ 651 pour indiquer que l'entrée est associée à la transition 83 et un champ 652 contenant la référence d'un programme 67, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment. De même, la table des vérifications 12 comporte une entrée 66 qui comprend respectivement un champ 661 pour indiquer que l'entrée est associée à la transition 83 et un champ 662 contenant la référence d'un programme 68, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment.

La figure 6d présente une réalisation de la table des actions 13. Ladite table comporte une entrée 71 qui comporte un champ 711 permettant d'indiquer que ladite entrée est associée à la transition 81. La même entrée 71 comporte un champ 712 contenant la référence d'un programme 75, implanté dans la mémoire de programmes, afin que le moteur de vérification puisse exécuter les actions systématiques associées à la transition 81. L'entrée 71 comporte en outre un champ 713 et un champ 714 contenant une référence nulle pour indiquer au moteur de vérification qu'aucune action positive ni négative n'est associée au franchissement de la transition 81. De la même manière, la table des actions 13 comporte une seconde entrée 72 comprenant les champs 721 à 724 pour indiquer au moteur de vérification que ladite entrée est associée à la transition 83, que le programme 74 est à exécuter comme action positive lors du franchissement de ladite transition et qu'aucune action systématique ou négative n'est à exécuter. L'absence d'entrée, au sein de la table des actions 13,

associée à la transition 85, indique qu'aucune action (systématique, positive ou négative) n'est à exécuter lors du franchissement ou du rejet du franchissement de ladite transition.

Grâce au dispositif et au procédé tels que décrits ci-dessus, le cycle de vie d'un objet électronique portatif est maîtrisé. Chaque transition d'états est irréversible et les vérifications faites lors de chaque demande de transitions garantissent une configuration mémoire de l'objet cohérente. En outre les actions systématiques, positives ou négatives permettent d'adapter le comportement dudit objet. Enfin, dans le cas où il est prévu d'autoriser une ou plusieurs transitions d'un ou plusieurs états de référence vers un état additif, le cycle de vie de l'objet peut être facilement enrichi, par exemple après que l'objet soit émis sur le marché, sans que le cycle de vie prédéfini (composé par une succession de transitions d'état de référence vers un autre état de référence) puisse être détourné.

Tout risque de fraude durant l'initialisation d'un objet électronique portatif ou d'erreur malencontreuse durant ladite initialisation est écarté tout en conservant grande adaptabilité du contrôle du cycle de vie de l'objet.

REVENDICATIONS

1. Dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif.

2. Dispositif selon la revendication 1, caractérisé en ce que les moyens de contrôle comportent des moyens d'autorisation et/ou interdiction de transitions d'état.

3. Dispositif selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que les moyens de contrôle comprennent des moyens de vérification du contenu de la mémoire volatile (3), des mémoires de données (5) et des mémoires de programmes (4) de l'objet électronique portatif en fonction de la transition d'états à effectuer.

4. Dispositif selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les moyens de contrôle comprennent:

- une table (11) des transitions d'état possibles;
- une table (12) des vérifications à effectuer par transition d'état possible;
- un moteur de vérification (9) exploitant lesdites tables.

5. Dispositif selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les moyens de contrôle comprennent en outre des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif.

6. Dispositif selon la revendication 5, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent une table (13) d'actions exploitable par ledit moteur de vérification (9).

7. Dispositif selon l'une quelconque des revendications 1 à 6, caractérisé en ce que les moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif comprennent en outre :

- une extension (16) de la table (11) des transitions d'état possibles;
- une extension (17) de la table (12) des vérifications à effectuer par transition d'état possible;

et en ce que le moteur de vérification (9) exploite lesdites extensions de tables (16, 17).

8. Dispositif selon l'une quelconque des revendications 5 à 7, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent en outre une extension (18) de la table (13) d'actions exploitable par le moteur de vérification (9).

9. Objet électronique portatif, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'il comporte le dispositif de contrôle du cycle de vie de l'objet, selon l'une des revendications 1 à 8.

10. Carte à puce, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'elle comporte le dispositif de contrôle du cycle de vie de la carte, selon l'une des revendications 1 à 8.

11. Procédé de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

ledit procédé étant mis en oeuvre, au sein de l'objet, à la suite d'une demande de transition d'états,

caractérisé en qu'il comprend :

- une étape (51, 511, 528, 521) de validation de l'autorisation de ladite demande;
- une étape (52, 512, 522) d'évaluation des vérifications associée à la transition demandée;
- une étape (57, 517, 527) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (51, 511, 528, 521) et, si les vérifications de la configuration de l'objet sont satisfaites (54, 514, 524).

12. Procédé selon la revendication 11, caractérisé en ce qu'il comprend en outre une étape (53, 513, 523) d'exécution d'actions systématiques.

13. Procédé selon l'une quelconque des revendications 11 ou 12 , caractérisé en ce qu'il comprend en outre une étape (56, 516, 526) d'exécution d'actions positives dans le cas où la transition demandée est autorisée (51, 511, 528, 521) et si les vérifications associées à la transition demandée sont satisfaites (54, 514, 524).

14. Procédé selon l'une quelconque des revendications 11 à 13, caractérisé en ce qu'il comprend en outre une étape (55, 515, 525) d'exécution d'actions négatives dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (54, 514, 524).

15. Procédé selon l'une quelconque des revendications 11 à 14, mis en œuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état de référence vers un second état de référence, caractérisé en qu'il comprend :

- une étape (51) de validation de l'autorisation de ladite demande consistant à analyser la table (11) des transitions possibles;
- une étape (52) d'évaluation des vérifications associée à la transition demandée consistant à exploiter une entrée (30) d'une table (12) des vérifications;
- une étape (57) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (51) et, si les vérifications de la configuration de l'objet sont satisfaites (54).

16. Procédé selon la revendication 15, caractérisé en ce qu'il comprend en outre une étape (53) d'exécution d'actions systématiques consistant à exploiter une entrée (400, 401, 404), correspondant à la transition demandée, d'une table (13) d'actions.

17. Procédé selon l'une quelconque des revendications 15 ou 16 , caractérisé en ce qu'il comprend en outre une étape (56) d'exécution d'actions positives consistant à exploiter une entrée (400, 402, 405), correspondant à la transition demandée, d'une table (13) d'actions, dans le cas où la transition demandée est autorisée (51) et si les vérifications associées à la transition demandée sont satisfaites (54).

18. Procédé selon l'une quelconque des revendications 15 à 17, caractérisé en ce qu'il comprend en outre une étape (55) d'exécution d'actions négatives consistant à exploiter une entrée (400, 403, 406), correspondant à la transition demandée, de la table (13) d'actions, dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (54).

19. Procédé selon l'une quelconque des revendications 11 à 14, ledit procédé étant mis en œuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état additif vers un second état additif, caractérisé en ce qu'il comprend :

- une étape (511) de validation de l'autorisation de ladite demande consistant à analyser une extension (16) de la table (11) des transitions possibles;

- une étape (512) d'évaluation des vérifications associée à la transition demandée consistant à exploiter une entrée (33) d'une extension (17) de la table (12) des vérifications;

- une étape (517) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (511) et, si les vérifications de la configuration de l'objet sont satisfaites (514).

20. Procédé selon la revendication 19, caractérisé en ce qu'il comprend en outre une étape (513) d'exécution d'actions systématiques en analysant une entrée (407, 408, 411), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions .

21. Procédé selon l'une quelconque des revendications 19 ou 20, caractérisé en ce qu'il comprend en outre une étape (516) d'exécution d'actions positives en analysant une entrée (407, 409, 412), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions demandée si :

- la transition demandée est autorisée (511)

- et, si les vérifications associées à la transition demandée sont satisfaites (514).

22. Procédé selon l'une quelconque des revendications 19 à 21, caractérisé en ce qu'il comprend en outre une étape (515) d'exécution d'actions négatives en analysant une entrée (407, 410, 413), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (514).

23. Procédé selon l'une quelconque des revendications 11 à 14, ledit procédé étant mis en œuvre, au sein de l'objet, à

la suite d'une demande de transition d'un état de référence vers un état additif, caractérisé en ce qu'il comprend :

- une étape (528) de validation de l'autorisation de d'une transition dudit état de référence vers un état additif en analysant la table (11) des transitions possibles;
- une étape (521) de validation de l'autorisation de d'une transition dudit état de référence vers ledit état additif en exploitant une extension (16) d'une table (11) des transitions possibles;
- une étape (522) d'évaluation des vérifications associée à la transition demandée en exploitant une entrée (33) d'une extension (17) d'une table (12) des vérifications;
- une étape (527) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (528, 521) et, si les vérifications de la configuration de l'objet sont satisfaites (524).

24. Procédé selon la revendication 23, caractérisé en ce qu'il comprend en outre une étape (523) d'exécution d'actions systématiques en exploitant une entrée (407, 408, 411), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions.

25. Procédé selon l'une quelconque des revendications 23 ou 24, caractérisé en ce qu'il comprend en outre une étape (526) d'exécution d'actions positives en exploitant une entrée (407, 409, 412), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions si:

- la transition demandée est autorisée (528, 521)
- et, si les vérifications associées à la transition demandée sont satisfaites (524).

26. Procédé selon l'une quelconque des revendications 23 à 25, caractérisé en ce qu'il comprend en outre une étape

(525) d'exécution d'actions négatives en exploitant une entrée (407, 410, 413), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (524).

27. Procédé selon l'une quelconque des revendications 11 à 26, caractérisé en ce que ledit procédé n'autorise pas le franchissement d'une transition d'état, d'un état additif vers un état de référence.

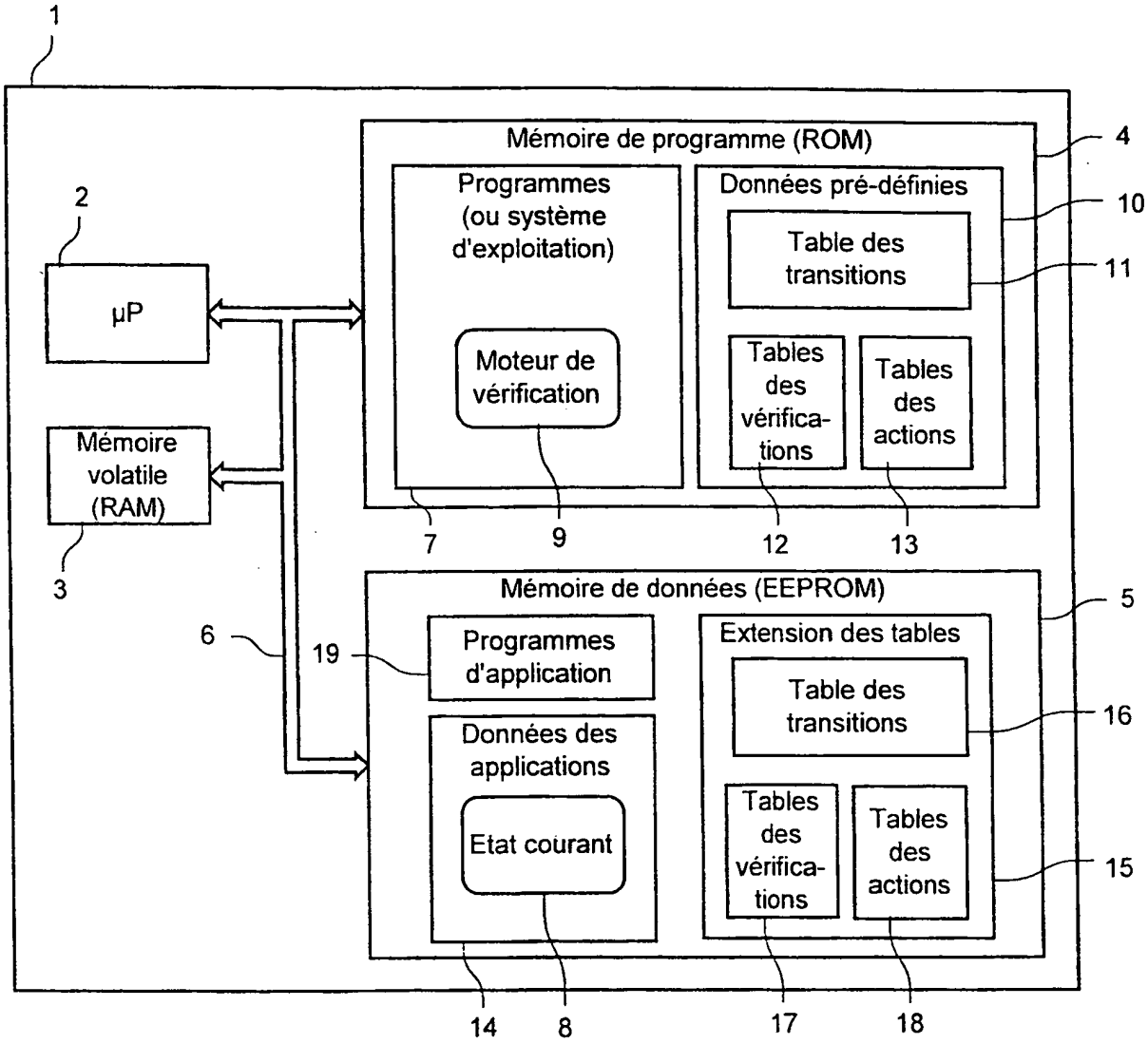

1
2
µP
Mémoire volatile (RAM)
3
Mémoire de programme (ROM)
4
Programmes (ou système d'exploitation)
Moteur de vérification
Données pré-définies
10
Table des transitions
11
Tables des vérifica-tions
Tables des actions
7
9
12
13
Mémoire de données (EEPROM)
5
6
19
Programmes d'application
Données des applications
Etat courant
Extension des tables
Table des transitions
16
Tables des vérifica-tions
Tables des actions
15
14
8
17
18

FIG. 1

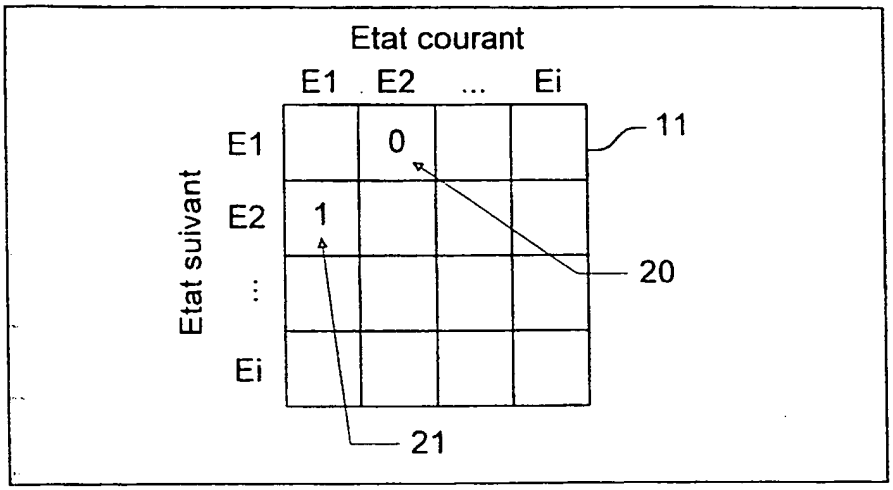

Etat courant
E1 E2 ... Ei
Etat suivant
E1
E2
Ei
0
1
11
20
21

FIG. 2a

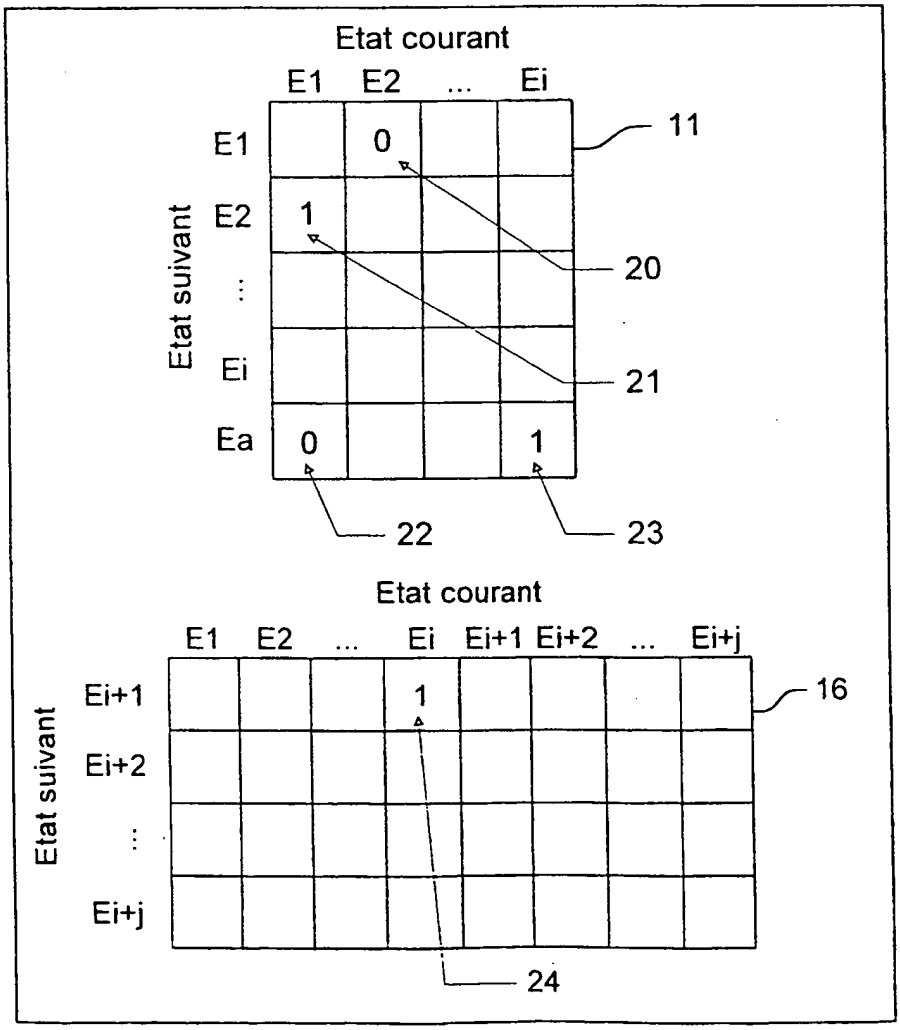

Etat courant
E1 E2 ... Ei
Etat suivant
E1
E2
Ei
Ea
0
1
11
20
21
22
23
Etat courant
E1 E2 ... Ei Ei+1 Ei+2 ... Ei+j
Etat suivant
Ei+1
Ei+2
Ei+j
1
16
24

FIG. 2b

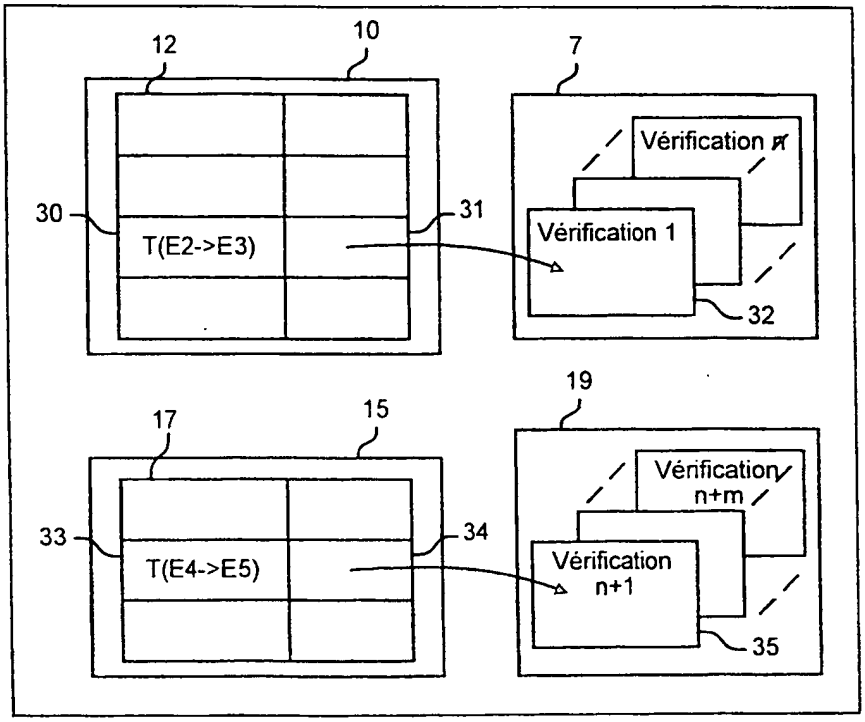

12
10
7
Vérification n
Vérification 1
30
31
T(E2->E3)
32
19
17
15
Vérification n+m
Vérification n+1
33
34
T(E4->E5)
35

FIG. 3

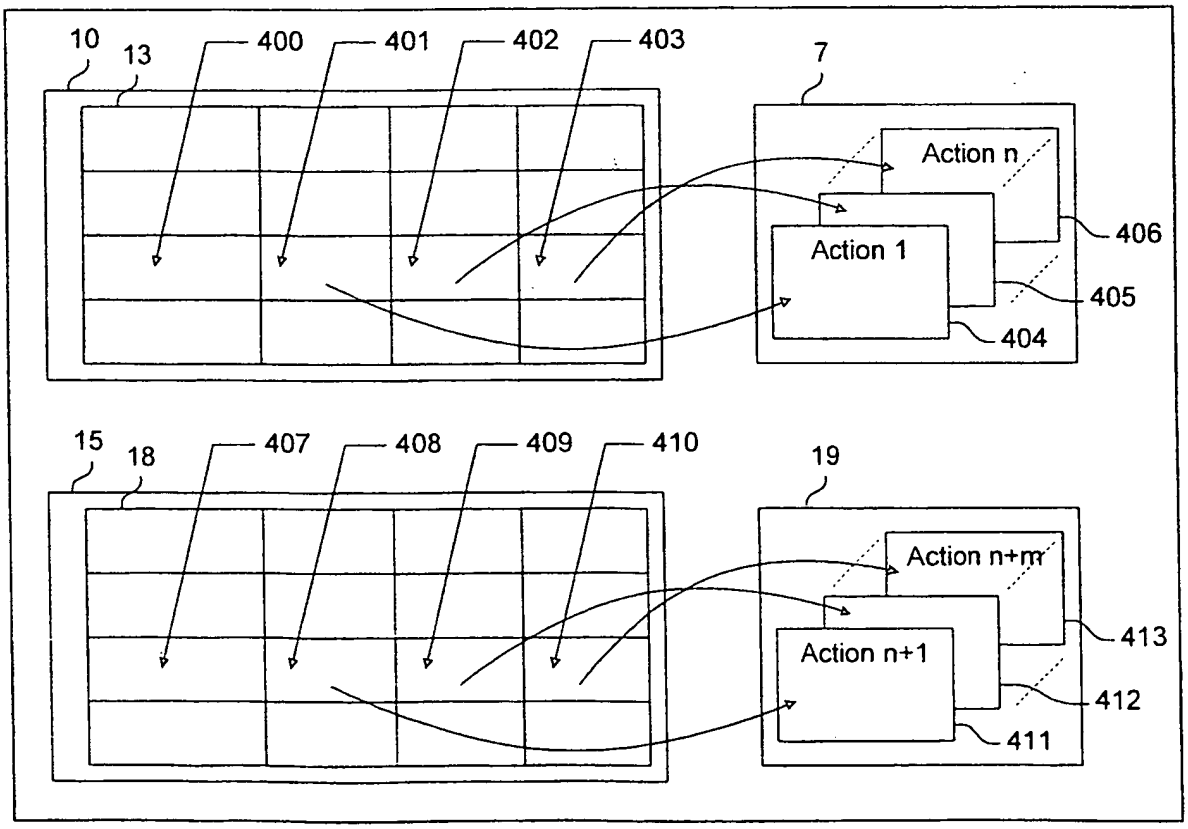

10
13
400
401
402
403
7
Action n
Action 1
406
405
404
15
18
407
408
409
410
19
Action n+m
Action n+1
413
412
411

FIG. 4

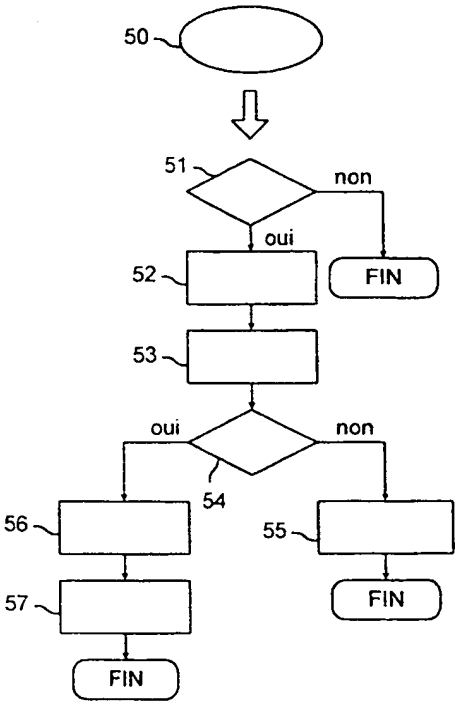


FIG. 5a

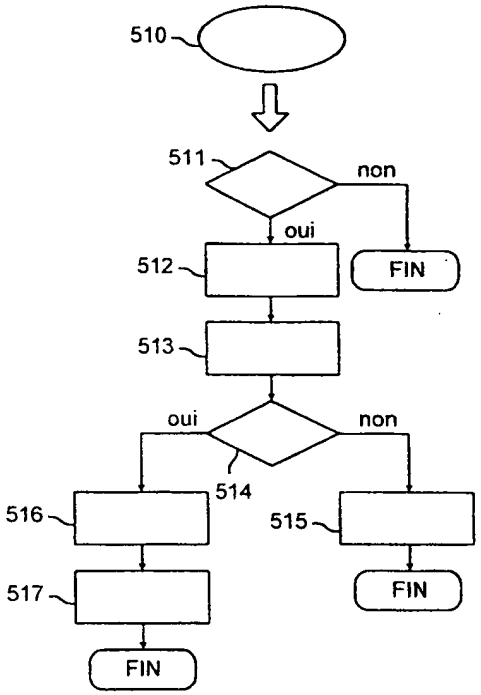


FIG. 5b

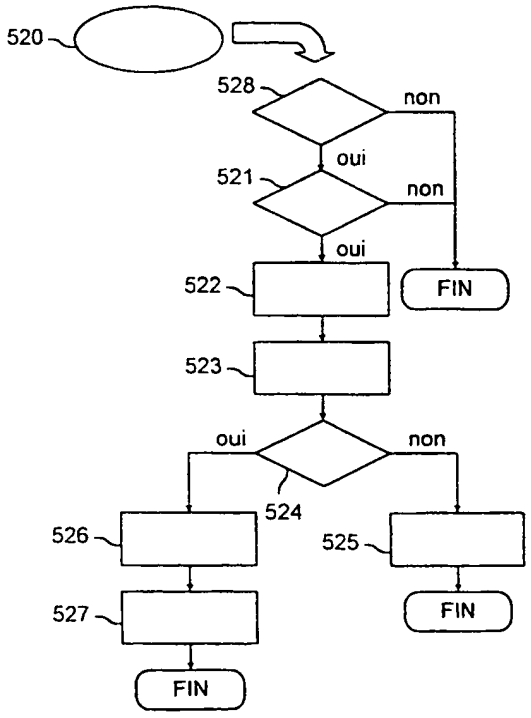


FIG. 5c

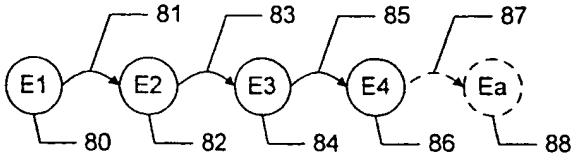


FIG. 6a

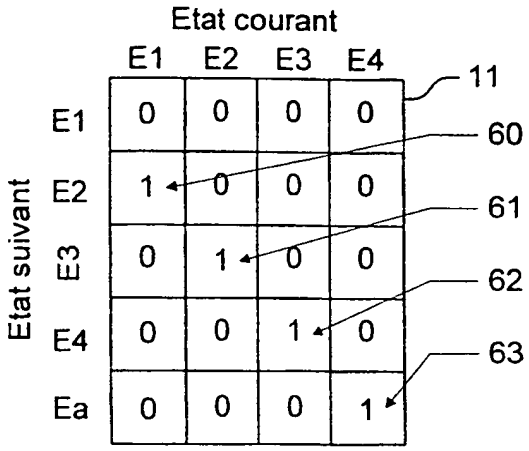


FIG. 6b

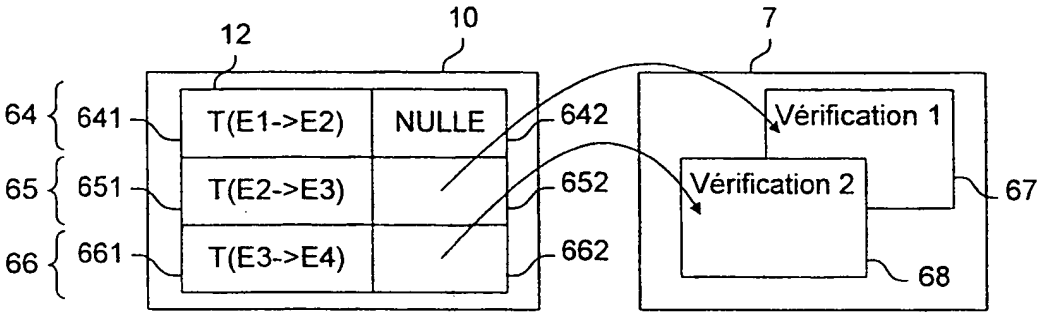


FIG. 6c

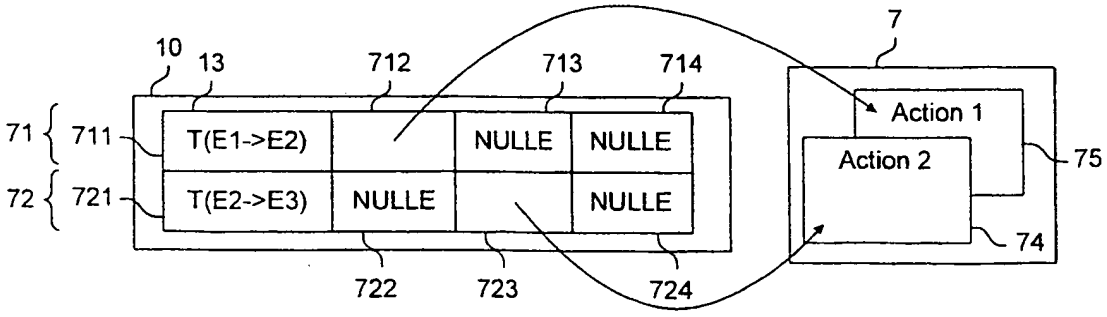


FIG. 6d

INTERNATIONAL SEARCH REPORT

Int. Application No
PCT/FR 99/02678

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 473 690 A (GRIMONPREZ GEORGES ET AL) 5 December 1995 (1995-12-05) the whole document	1-27
A	WO 98 09257 A (GEMPLUS CARD INT) 5 March 1998 (1998-03-05) page 14, line 4 -page 20, line 19	1,11
A	EP 0 583 006 A (MATSUSHITA ELECTRIC IND CO LTD) 16 February 1994 (1994-02-16) column 3, line 35 -column 7, line 5	1,11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2000	25/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Goossens, A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTER TIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/FR 99/02678

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5473690 A	05-12-1995	FR 2673476 A	04-09-1992
		DE 69205425 D	16-11-1995
		DE 69205425 T	21-03-1996
		EP 0589884 A	06-04-1994
		ES 2082451 T	16-03-1996
		WO 9213322 A	06-08-1992
		JP 6504862 T	02-06-1994
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AU 4842897 A	19-03-1998
		CA 2233217 A	05-03-1998
		EP 0858644 A	19-08-1998
EP 0583006 A	16-02-1994	JP 2502894 B	29-05-1996
		JP 6060235 A	04-03-1994
		JP 6131517 A	13-05-1994
		DE 69320900 D	15-10-1998
		DE 69320900 T	28-01-1999
		KR 9706648 B	29-04-1997
		US 5408082 A	18-04-1995

RAPPORT DE RECHE .IE INTERNATIONALE

Der .ernationale No
PCT/FR 99/02678

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/073 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 473 690 A (GRIMONPREZ GEORGES ET AL) 5 décembre 1995 (1995-12-05) le document en entier	1-27
A	WO 98 09257 A (GEMPLUS CARD INT) 5 mars 1998 (1998-03-05) page 14, ligne 4 -page 20, ligne 19	1,11
A	EP 0 583 006 A (MATSUSHITA ELECTRIC IND CO LTD) 16 février 1994 (1994-02-16) colonne 3, ligne 35 -colonne 7, ligne 5	1,11

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 janvier 2000	25/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Goossens, A

1

RAPPORT DE R ¡ERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den e Internationale No
PCT/FR 99/02678

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5473690 A	05-12-1995	FR 2673476 A	04-09-1992
		DE 69205425 D	16-11-1995
		DE 69205425 T	21-03-1996
		EP 0589884 A	06-04-1994
		ES 2082451 T	16-03-1996
		WO 9213322 A	06-08-1992
		JP 6504862 T	02-06-1994
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AU 4842897 A	19-03-1998
		CA 2233217 A	05-03-1998
		EP 0858644 A	19-08-1998
EP 0583006 A	16-02-1994	JP 2502894 B	29-05-1996
		JP 6060235 A	04-03-1994
		JP 6131517 A	13-05-1994
		DE 69320900 D	15-10-1998
		DE 69320900 T	28-01-1999
		KR 9706648 B	29-04-1997
		US 5408082 A	18-04-1995

Translation of the international application as published

A METHOD AND DEVICE FOR CONTROLLING THE LIFE CYCLE OF A PORTABLE OBJECT, NOTABLY A SMART CARD

The invention concerns portable electronic objects such as electronic microcircuit cards, known as smart cards, which, connected to electronic devices to enable the latter to perform particular functions in the context of one or more applications, require their life stages to be controlled. The said cards are in fact generally used in applications (banking, communication, identity, health etc) requiring a high degree of security against fraudulent usage. The invention applies more generally to any independent on-board system provided with a processing unit and program and data memories.

In the world of smart cards it is known that the latter result from assembling a component (generally comprising a microprocessor in relationship with memories via communication buses), a module (produced by means of a conductive metal) to which the said

component is connected (in the context of a so-called contact smart card) to enable the said component to be connected to an electronic reading and/or writing device (or coupler) and a card body or more generally a support on which the module/component assembly is integrated. In the context of a so-called contactless smart card, the said module is replaced by an antenna and the assembly formed by the component and the said antenna is integrated within the said support.

The life of a smart card can generally be broken down into two sets of stages following each other, corresponding respectively to the manufacture and use of the said card. Putting together the two sets of stages forms a life cycle of the said card. The manufacture of a smart card (with or without contact) consists of several stages.

This is because it is first of all necessary to have an electronic component which is initialised, insulated and then connected to a module. The said component and the module to which it is connected are subsequently integrated on or within a support (generally a plastic card body) itself printed for the purpose of identification or advertising. Subsequently the smart card thus obtained is initialised or programmed in order to meet the conditions of use in the context of applications.

The second set of life stages of a smart card corresponds to its use. This set can itself be divided into several stages, each corresponding, for example, to the implantation or elimination of services offered

by the smart card to the user according to his profile, for example.

In addition different participants (component manufacturer, smart card manufacturer, card personalisation centre, card issuer or card carrier) act during the different stages of manufacture and use of a smart card. Thus the components are supplied and sometimes partly initialised by electronic component manufacturers on a silicon wafer. This phase corresponds to the step of manufacturing the component. The following step is the embedding phase carried out by the smart card manufacturer. It includes the insulation of a component from the silicon wafer, the connection of the said component to a module (or antenna), and the integration of the assembly on the support or card body. There follows the preparation of the application structure present in the electrically programmable memory of the component. This is the electrical personalisation stage which is carried out by the manufacturer of the smart cards or by a personalisation centre or a third party specialising in personalisation of cards or by the issuer himself who is ultimately responsible for the distribution of the cards on the market. This electrical personalisation phase can therefore be broken down into as many stages as there are players or intermediaries. Subsequently, during the use of the smart card, we have seen previously that it can be advantageous to distinguish several stages along with the change in the profile of the card user for example.

Whatever the case, it is therefore important to rigorously monitor the life stages of a card in order to know at any time the current stage of the said card within its life cycle. In addition, it is essential on the one hand for access to the electrically programmable memory of a card component in write or read mode to be protected during the exchange of the said card (or component) during the different participants and on the other hand for access to the said memory to be limited as the life stages of the card mentioned above follow each other, by activating or deactivating services for example. Finally, it is also sometimes necessary to validate the application context of the smart card before the carrier thereof uses it on the market. For example, a person issuing a smart card of the electronic purse type must be certain that the balance of the said card is indeed zero before issuing the card.

In order to attempt to meet these requirements, different solutions are used at the present time. Certain solutions are purely external to the smart card (physical security at the premises where the said card is manufactured, use of transportation means which are themselves made secure etc). Other solutions complementary to the first, but this time internal or implanted in the card, are also generally used. Use is thus made of secrets for protecting access to the component memory in read/write mode and also logic indicators for irreversibly monitoring the different life stages of the card. For this purpose, bits within

a non-erasable memory of the component of the smart card are positioned at the active state at the end of the different life stages of the card (manufacture and initialisation of the component by the manufacturer of the said component, embedding and initialisation of the card memory by the smart card manufacturer, preparation of the application structure of the smart card memory by the personalisation centre or the card issuer etc). According to these indicators, the program (or operating system) executed by the microprocessor of the smart card component, implanted within one of the memories of the said card component, adapts its behaviour as the life stages of the said card follow each other. Thus functions can be modified, added or eliminated.

Whatever the solutions used at the present time, they are all based on the fact that the different players involved in the manufacture of a card are trusted third parties. Only persons liable to intercept components or cards during their transfer between two of the different players are deemed to be "potential fraudsters" and the solutions disclosed above make it possible to be free of them. The adaptation of the operating system of the card according to irreversible indicators affords a not insignificant advantage. Thus, if the manufacturers of the components or cards inscribe systems data or secrets, the card issuer will for example not be able to dispense freely with the said secrets or modify the said system data. However, this solution does not

resolve the problem of a fraudulent initialisation of the card or an inopportune error during the said initialisation, carried out by one of the participants.

The invention proposes to remedy the drawbacks of the current state of the art. In particular, the invention consists of providing the operating system of a smart card with software means enabling the said operating system to control an irreversible change in life stage of the said card according to a set of checks on the content of the memories of this same smart card. In addition the invention makes provision, during a change in life stage, for the operating system of the card to be able to automatically trigger actions for adapting the services offered by the said operating system of the said card.

To this end, the invention concerns a device for controlling the life cycle of a portable electronic object, the life cycle consisting of a succession of state transitions, the said states determining the services offered by the object, the said object comprising a processing unit, a volatile memory, program memories and data memories, each of these memories having a content defining a plurality of configurations, characterised in that it has means of controlling the transition from a first state to a second state of the portable electronic object.

According to other characteristics of the device according to the invention:

- the control means have:

- means of enabling and/or inhibiting state transitions to be effected;

- means of checking the content of the volatile memory, of the data memories and of the program memories of the portable electronic object according to the state transition to be effected;

- means for triggering actions during the processing of a request to effect a state transition.

In addition, the invention concerns a portable electronic object, which may notably be a smart card, containing the said life cycle control device.

Moreover, the invention concerns a method of controlling the life cycle of a portable electronic object, the said method being implemented within the object following a state transition request,

characterised in that it comprises:

- a step of validating the enabling of the said request;

- a step of evaluating the checks associated with the requested transition;

- a step of modifying the current state of the object if and only if the requested transition is enabled and if the checks on the configuration of the object are satisfied.

According to other characteristics, the method possibly also comprises:

- a step of executing systematic actions;

- a step of executing positive actions in the case where the requested transition is enabled and if the

checks associated with the requested transition are satisfied;

- a step of executing negative actions in the case where the checks associated with the requested transition are not satisfied.

The invention will be understood more clearly from a reading of the following description and an examination of the figures which accompany it. These are given only as an indication and are in no way limitative of the invention.

The figures show:

- Figure 1: a component of a smart card provided with a state transition check device;

- Figures 2a and 2b: a detailed representation of a state transition table;

- Figure 3: a detailed representation of a transition check table;

- Figure 4: a detailed representation of an action table;

- Figure 5: a description of the steps implemented in the method used by the transition check device;

- Figures 6a to 6d: the particularities implemented in the case of an example of a smart card of the electronic purse type.

In the invention, the term reference state will refer to a state from which it is possible to switch to another state following the crossover of a transition described in the table of transitions, located in the program memory. As described below, it is possible to add new states and therefore new transitions after the

step of manufacturing the component has taken place. In this case, additive states will be spoken of in order to characterise these in contradistinction to reference states. In addition, the state in which the on-board system is will be referred to as the current state.

Figure 1 shows a component 1, of a smart card, provided with a transition check device according to the invention. The component has a processing unit 2 or a microprocessor in relationship with memories 3, 4 and 5 via a communication bus 6. A non-erasable program memory 4 (or a ROM) has on the one hand a program area 7, the said programs (or on-board system) being able to be executed by the said processing unit and on the other hand a predefined data area 10 which contains constants used by the said operating system. Amongst the said constants of the area 10, the operating system 7, containing a program referred to as a check engine 9, uses a table of transitions 11 which makes it possible to specify the states to which it is possible to gain access from the current state, a check table 12 which makes it possible to associate with each state transition checks relating to the content of the memories 3, 4 and/or 5. In a variant, the check engine 9 can automatically trigger actions when a transition is crossed over or this crossover is rejected. For this purpose, the area 10 of the program memory contains a table of actions 13 which makes it possible to associate actions to be performed with each possible state transition.

A volatile memory 3 (or RAM, standing for Random Access Memory in English) enables the processing unit 2 to temporarily store results or secrets issuing from calculations described by the programs implanted in the program memory 4. The content of the memory 3 is erased each time the component 1 is powered up or each time resetting thereof is requested.

A data memory 5, electrically erasable, generally using EEPROM technology (standing for Electrically Erasable Programmable Read Only Memory in English) has an area 14 containing the variable data necessary for executing the programs 7. This area 14 contains notably a data item 8 referred to as the "current state" making it possible to store the current state of the portable electronic object. The data memory 5 also has an area 15 comprising optionally extensions to the tables 11 to 13 in the case where it is necessary to add states to the reference states. The area 15 then contains an extension to the table of transitions 16 and an extension to the check table 17 and may include an extension to the table of actions 18 if it is wished to associate actions with the new additive state transitions, as seen previously with regard to table 13. In the case of adding states with respect to the reference states, it is sometimes essential to enhance the operating system 7. For this purpose, the memory 5 can also include an area 19 which contains the additional programs which will be executed in their turn by the processing unit 2.

Figure 2a shows a possible use of the table of transitions 11. If it is assumed that i reference states are counted, it is possible to imagine a transition table comprising i columns and i rows. The columns correspond to the reference states which, at a given time, can be the current state. The first i rows correspond to the reference states to which access can be gained from the current state. Thus the value of a box in the table of transitions 11 corresponding to the intersection of a row and column in the said table makes it possible to code either the absence of an enabled transition (zero value for example - this is the case with the transition 20) or the enabling of a transition (non-zero value - this is the case with the transition 21). In the case of an enabled transition, the transition check engine searches within the check table 12 the checks to be made in order to accept or reject the crossover of the requested transition.

Figure 2b also shows a possible implementation of a transition table in the case where it is possible to add states (additive states) to the reference states. The table of transitions includes an additional line compared with Figure 2a. The (i+1)th line makes it possible to specify if transitions from a current reference state to an additive state are enabled. Thus the value of the box 22 indicates an inhibited transition from a reference state to an additive state. The box 23 indicates that it will be possible to switch from the reference state Ei to an additive state. An extension 16 to the table of transitions is then

necessary. The latter has j lines corresponding to j additive states to which it is possible to gain access from the (i+j) possible current states represented by the (i+j) columns of the extension 16 to the table of transitions. Thus the combination of the box 23 in the table of transitions and the box 24 of the extension 16 of the table of transitions indicates to the check engine that it is possible to switch from the reference state Ei to the additive state E(i+1).

Figure 3 shows a use of the check table. The check table 12 is located within the area 10 of the predefined data of the memory 4. Each enabled transition has an entry in the said table. An entry comprises a field 30 for identifying the transition and a field 31 containing a reference (or address) to a program 32 of the operating system 7. The check engine 9 can thus make the processing unit 2 execute the required controls for accepting the crossover of the transition. Figure 3 also illustrates a structure of an extension 17 to the check table. In the same way as with the table 12, the extension to the check table 17 has one entry per possible transition. Each entry comprises two fields, a field 33 for identifying the transition and a field 34 containing a reference (or address) of a program 35 of the operating system or, as shown by Figure 3, an additional program located in the data memory 5 (in the area 19).

Figure 4 shows a representation of the table of actions 13 located in the area 10 of the predefined data of the program area 4. At the time of a

transition crossover request, it is possible to trigger actions. These can be of three types: systematic action, positive action (that is to say dependent on the fact that the checks are satisfactory) or negative action (that is to say dependent on the fact that the checks are not satisfactory). Figure 4 shows that, at each enabled transition, there is an entry in the table of actions 13. This entry comprises four fields. The first field 400 identifies the transition. The other three fields 401, 402 and 403 each contain a reference or address of a program 404, 405 or 406 of the operating system. The field 401 is dedicated to a systematic action, the field 402 to a positive action and the field 403 to a negative action. Figure 4 also shows an extension 18 to the table of actions. This table 18 is located in the area 15 of the data memory 5 of the component 1. In the same way as with the table of actions 13, the extension to the table of actions 18 comprises one entry per possible transition. An entry comprises four fields. The first field 407 identifies the transition. The other three fields 408, 409 and 410 each contain a reference or address of a program 411, 412 or 413 of the operating system or, as shown by Figure 4, programs located in the area 19 of the data memory 5 of the component 1. The field 408 is dedicated to a systematic action, the field 409 to a positive action and the field 410 to a negative action.

Figure 5a describes the method for validating or rejecting the crossover of a state transition, from a first reference state to another reference state. The

request for crossover of a transition can be formulated following an instruction from the card manufacturer or by any other player in the life cycle of the smart card. The said request can also be formulated directly by the card itself, for example through an action associated with a transition. In the context of Figure 5a, the current reference state is the state Ei. The instruction 50 to switch from the state Ei to the state Ej is formulated. Step 51 consists of checking, within the table of transitions 11, that the transition from the state Ei to the state Ej is enabled. Where this transition is inhibited, the transition crossover request 50 is rejected. The current state remains the state Ei. On the other hand, if the transition is enabled, the check engine 9 executes the checks associated with the said transition. For this purpose the check engine evaluates the entry in the check table 12 dedicated to the transition T(Ei→Ej). The execution of said checks corresponds to step 52 of the method. The check engine 9 executes the systematic actions associated with the transition T(Ei→Ej) according to the entry in the table of actions 13 dedicated to the said transition (step 53). If the checks 54 required at the time of the request for crossover of the transition 50 are not satisfactory, the current state remains unchanged. According to the entry in the table of actions 13 associated with the transition T(Ei→Ej) the check engine executes the negative actions (step 55 of the method). The performance of the method is then terminated. On the other hand, if the checks 54 are

satisfactory, then the current state becomes the state Ej (step 56 of the method). The positive actions are then executed (step 57 of the method) according to the state of the entry in the table of actions 13 associated with the transition T(Ei→Ej). The performance of the method is terminated.

Figure 5b describes the method for validating or rejecting the crossover of a state transition, from a first additive state to another additive state. The current additive state is the state Ei. The instruction 510 to switch from the additive Ei to the additive state (or reference state) Ej is formulated. Step 511 of the method consists of checking within the extension to the table of transitions 16 that the transition from state Ei to state Ej is enabled. Where this transition is inhibited, the transition crossover request 510 is rejected. The current state remains the state Ei. On the other hand, if the transition is enabled, the check engine 9 executes the checks associated with the said transition. For this purpose, the check engine evaluates the entry in the extension to the check table 17 dedicated to the transition T(Ei→Ej). The execution of the said checks constitutes step 512 of the method. The check engine 9 executes the systematic actions associated with the transition T(Ei→Ej) according to the entry in the extension to the table of actions 18 dedicated to the said transition (step 513 of the method). If the check 514 required at the time of the transition crossover request 510 is not satisfactory, the current state remains unchanged.

According to the entry in the extension to the table of actions 18 associated with the transition T(Ei→Ej), the check engine 9 executes the negative actions (step 515 of the method). The performance of the method is then terminated. On the other hand, if the checks 514 are satisfactory, the current state becomes state Ej (step 516 of the method). The positive actions are then executed (step 517 of the method) according to the state of the entry in the extension to the table of actions 18 associated with the transition T(Ei→Ej). The performance of the method is terminated.

Figure 5c describes the method for validating or rejecting the crossover of a state transition, from a reference state to an additive state. The current reference state is the state Ei. The instruction 520 to switch from the reference state Ei to the additive state Ej is formulated. Step 528 of the method consists of checking, within the table of transitions 11, that a transition from the current reference Ei to an additive state is enabled. If such a transition is inhibited, the method is terminated. The current state remains unchanged. On the other hand, if a transition from the said reference state to an additive state is enabled, the check engine runs steps 521 to 527 of the method, respectively identical to steps 511 to 517 described in relation to Figure 5b.

An example of an application in the field of electronic purses is presented in relation to Figures 6a to 6d. The said application makes it possible to pay for purchases by means of "electronic money" stored

in a smart card, instead of paying in cash. The use of such a technique requires a management of the cards which is as secure as that which would have been imposed by the use of cash. It is necessary for example to avoid the creation of paper money. The security of an electronic purse smart card is generally based on keys stored within the smart card allowing secure transactions using cryptography. Such a card has an operating system offering a set of commands and services for crediting or debiting money. At the start of the life cycle of the electronic purse smart card, the said smart card is not initialised. It contains no information. Figure 6a shows the predefined reference states:

- State E1 "blank card" (referenced 80): only test commands for validating the behaviour of the data memory 5 are available (verification that the EEPROM technology memory boxes can be correctly written to and erased);

- State E2 "tested card" (referenced 82): the test commands are no longer available. In their turn commands generally known as "physical commands" (allowing access in write mode by means of a physical addressing independently of any logic structure of the file type for example) are available. They make it possible to initialise the card (writing in the area 14 of the data memory of the logic constituents necessary for the functioning of the application, that is to say files, balances etc);

- State E3 "initialised card" (referenced 84): the physical commands are no longer available. Logic commands for personalising the card (addition of new logic structures and initialisation data in the said structures) can be used. In addition, a recovery mechanism is activated so that the smart card does not lose the coherence of these data when it is powered down during the execution of one of the said logic commands;

- State E4 "personalised card" (referenced 86): the logic commands specific to the electronic purse application (debit/credit) are activated.

The set of available commands changes according to the life stage in which the smart card is situated. Information stored in data memory enables the operating system to know the state in which the smart card is situated. Figure 6a also shows that, in the context of a card of the electronic purse type, all the transitions between reference states must be crossed successively (from state E1 to state E4), and this irreversibly. Any other transition is inhibited. Only the possibility of subsequently using additive states 88 is offered. This possible transition is referenced 87. The operating system according to the current state allows only a set of commands specific to each reference state.

The checks and actions to be triggered when a transition is crossed are described as follows:

- Transition from state E1 to state E2 (denoted T(E1→E2) and referenced 81):

- Check: none
- Systematic action:

erasure of the data memory in order to prevent a fraudster leaving therein data which can be interpreted by the card operating system;

- Transition from state E2 to state E3 (denoted T(E2→E3) and referenced 83):
  - Check:
    - integrity of the data written in the data memory with the physical commands (validation of a redundancy code by data);
    - verification of the blank state of the memory apart from the said data;
  - Positive action:
    - activation of the recovery mechanism;
- Transition from state E3 to state E4 (denoted T(E3→E4) and referenced 85):
  - Verification:
    - nullity of the balance of the electronic purse
  - Action: none
- Transition from state E4 to an additive state (denoted T(E4→Eadd) and referenced 87):
  - Verification: none
  - Action: none

Figures 6b to 6d illustrate respectively an embodiment of a table of transitions 11, a check table 12 and a table of actions 13, according to the invention. The table of transitions 11 as described in

relation to Figure 6b makes it possible to enable only the transitions 81, 83, 85 and 87. For this, only the boxes 60 to 63 in the said table contain a non-zero value. The other boxes in the table of transitions contain a zero value in order to indicate that any other transition is inhibited. The check table as presented through Figure 6c makes it possible to associate the checks to be satisfied for enabling the crossover of the transitions 81, 83, 85 and 87, the said transitions enabled by the table of transitions 11 (Figure 6b). Thus the entry 64 in the check table 12 includes a field 641 for identifying the fact that the said entry is dedicated to the transition 81. The entry 64 also includes a field 642 containing a zero reference in order to indicate that no check is requested in order to allow the crossover of the transition 81. In a variant, the transition 81 has no associated entry. This variant is illustrated later in the case of the table of actions. The check table 12 has an entry 65 which comprises respectively a field 651 for indicating that the entry is associated with the transition 83 and a field 652 containing the reference of a program 67, located in the program memory, so that the check engine can make the checks described above. Likewise, the check table 12 has an entry 66 which comprises respectively a field 661 for indicating that the entry is associated with the transition 83 and a field 662 containing the reference of a program 68, located in the program memory, so that

the check engine can make the previously described checks.

Figure 6d presents an embodiment of the table of actions 13. The said table has an entry 71 which includes a field 711 for indicating that the said entry is associated with the transition 81. The same entry 71 has a field 712 containing the reference of a program 75, located in the program memory, so that the check engine can execute the systematic actions associated with the transition 81. The entry 71 also has a field 713 and a field 714 containing a zero reference in order to indicate to the check engine that no positive or negative action is associated with the crossover of the transition 81. In the same way, the table of actions 13 has a second entry 72 comprising the fields 721 to 724 in order to indicate to the check engine that the said entry is associated with the transition 83, that the program 74 is to be executed as a positive action when the said transition is crossed and that no systematic or negative action is to be executed. The absence of entry, within the table of actions 13, associated with the transition 85, indicates that no action (systematic, positive or negative) is to be executed at the time of crossover or rejection of crossover of the said transition.

By means of the device and method as described above, the life cycle of a portable electronic object is controlled. Each state transition is irreversible and the checks made at the time of each transition request guarantee a coherent memory configuration for

the object. In addition, the systematic, positive or negative actions make it possible to adapt the behaviour of the said object. Finally, in the case where provision is made for enabling one or more transitions from one or more reference states to an additive state, the life cycle of the object can easily be enhanced, for example after the object is issued on the market, without the predefined life cycle (composed of a succession of transitions from one reference state to another reference state) being able to be diverted.

Any risk of fraud during the initialisation of a portable electronic object or of an inopportune error during the said initialisation is removed whilst preserving great adaptability of control of the life cycle of the object.

CLAIMS

1. A device for controlling the life cycle of a portable electronic object, the life cycle being determined by a succession of state transitions, the said states determining the services offered by the object, the said object comprising a processing unit (2), a volatile memory (3), program memories (4) and data memories (5), each of these memories (3, 4, 5) having a content defining a plurality of configurations,

characterised in that it has means of controlling the transition from a first state to a second state of the portable electronic object.

2. A device according to Claim 1, characterised in that the control means have means of enabling and/or inhibiting state transitions.

3. A device according to either one of Claims 1 or 2, characterised in that the control means comprise means of checking the content of the volatile memory (3), the data memories (5) and the program memories (4) of the portable electronic object as a function of the state transition to be effected.

4. A device according to any one of Claims 1 to 3, characterised in that the control means comprise:

- a table (11) of possible state transitions;
- a table (12) of the checks to be made per possible state transition;
- a check engine (9) using the said tables.

5. A device according to any one of Claims 1 to 4, characterised in that the control means also comprise means for triggering actions during the processing of a request for a transition from a first state to a second state of the portable electronic object.

6. A device according to Claim 5, characterised in that the means for triggering actions during the processing of a request for transition from a first state to a second state of the portable electronic object comprise a table (13) of actions which can be used by the said check engine (9).

7. A device according to any one of Claims 1 to 6, characterised in that the means of controlling the transition from a first state to a second state of the portable electronic object also comprise:

- an extension (16) to the table (11) of possible state transitions;

- an extension (17) to the table (12) of checks to be made per possible state transition;

and in that the check engine (9) uses the said table extensions (16, 17).

8. A device according to any one of Claims 5 to 7, characterised in that the means for triggering actions during the processing of a request for transition from a first state to a second state of the portable electronic object also comprise an extension (18) to the table (13) of actions which can be used by the check engine (9).

9. A portable electronic object having a processing unit (2), a volatile memory (3), program memories (4) and data memories (5), characterised in that it includes the device for controlling the life cycle of the object, according to one of Claims 1 to 8.

10. A smart card having a processing unit (2), a volatile memory (3), program memories (4) and data memories (5), characterised in that it includes the device for controlling the life cycle of the object, according to one of Claims 1 to 8.

11. A method of controlling the life cycle of a portable electronic object, the life cycle being determined by a succession of state transitions, the said states determining the services offered by the object, the said object comprising a processing unit (2), a volatile memory (3), program memories (4) and data memories (5), each of these memories (3, 4, 5) having a content defining a plurality of configurations,

the said method being implemented, within the object, following a state transition request,

characterised in that it comprises:

- a step (51, 511, 528, 521) of validation of the enabling of the said request;

- a step (52, 512, 522) of evaluating the checks associated with the requested transition;

- a step (57, 517, 527) of modifying the current state of the object if and only if the requested transition is enabled (51, 511, 528, 521) and if the

checks on the configuration of the object are satisfied (54, 514, 524).

12. A method according to Claim 11, characterised in that it also comprises a step (53, 513, 523) of executing systematic actions.

13. A method according to either one of Claims 11 or 12, characterised in that it also comprises a step (56, 516, 526) of executing positive actions in the case where the requested transition is enabled (51, 511, 528, 521) and if the checks associated with the requested transition are satisfied (54, 514, 524).

14. A method according to any one of Claims 11 to 13, characterised in that it also comprises a step (55, 515, 525) of executing negative actions in the case where the checks associated with the requested transition are not satisfied (54, 514, 524).

15. A method according to any one of Claims 11 to 14, implemented within the object, following a request for transition from a first reference state to a second reference state, characterised in that it comprises:

- a step (51) of validating the enabling of the said request consisting of analysing the table (11) of possible transitions;

- a step (52) of evaluating the checks associated with the requested transition consisting of using an entry (30) in a table (12) of checks;

- a step (57) of modifying the current state of the object if and only if the requested transition is enabled (51) and if the checks on the configuration on the object are satisfied (54).

16. A method according to Claim 15, characterised in that it also comprises a step (53) of executing systematic actions consisting of using an input (400, 401, 404), corresponding to the requested transition, of a table of actions (13).

17. A method according to either one of Claims 15 or 16, characterised in that it also comprises a step (56) of executing positive actions consisting of using an entry (400, 402, 405), corresponding to the requested transition, in a table (13) of actions, in the case where the requested transition is enabled (51) and if the checks associated with the requested transition are satisfied (54).

18. A method according to any one of Claims 15 to 17, characterised in that it also comprises a step (55) of executing negative actions consisting of using an entry (400, 403, 406), corresponding to the requested transition, in the table (13) of actions, in the case where the checks associated with the requested transition are not satisfied (54).

19. A method according to any one of Claims 11 to 14, the said method being implemented within the object, following a request for transition from a first additive state to a second additive state, characterised in that it comprises:

- a step (511) of validating the enabling of the said request consisting of analysing an extension (16) of the table (11) of possible transitions;

- a step (512) of evaluating the checks associated with the requested transition consisting of using an

entry (33) in an extension (17) to the table (12) of checks;

- a step (517) of modifying the current state of the object if and only if the requested transition is enabled (511) and if the checks on the configuration of the object are satisfied (514).

20. A method according to Claim 19, characterised in that it also comprises a step (513) of executing systematic actions by analysing an entry (407, 408, 411), corresponding to the requested transition, with an extension (18) to a table (13) of actions.

21. A method according to either one of Claims 19 or 20, characterised in that it also comprises a step (516) of executing positive actions by analysing an entry (407, 409, 412), corresponding to the requested transition, in an extension (18) of a requested table (13) of actions if:

- the requested transition is enabled (511)

- and if the checks associated with the requested transition are satisfied (514).

22. A method according to any one of Claims 19 to 21, characterised in that it also comprises a step (515) of executing negative actions by analysing an entry (407, 410, 413), corresponding to the requested transition, in an extension (18) to a table (13) of actions in the case where the checks associated with the requested transition are not satisfied (514).

23. A method according to any one of Claims 11 to 14, the said method being implemented, within the object, following a request for transition from a

reference state to an additive state, characterised in that it comprises:

- a step (528) of validating the enabling of a transition from the said reference state to an additive state by analysing the table (11) of possible transitions;

- a step (521) of validating the enabling of a transition from the said reference state to the said additive state using an extension (16) to a table (11) of possible transitions;

- a step (522) of evaluating the checks associated with the requested transition using an entry (33) in an extension (17) to a table (12) of checks;

- a step (527) of modifying the current state of the object if and only if the requested transition is enabled (528, 521) and if the checks on the configuration of the object are satisfied (524).

24. A method according to Claim 23, characterised in that it also comprises a step (523) of executing systematic actions using an entry (407, 408, 411), corresponding to the requested transition, in an extension (18) to a table (13) of actions.

25. A method according to either one of Claims 23 or 24, characterised in that it also comprises a step (526) of executing positive actions using an entry (407, 409, 412), corresponding to the requested transition, in an extension (18) to a table (13) of actions if:

- the requested transition is enabled (528, 521)

- and if the checks associated with the requested transition are satisfied (524).

26. A method according to any one of Claims 23 to 25, characterised in that it also comprises a step (525) of executing negative actions using an entry (407, 410, 413), corresponding to the requested transition, in an extension (18) to a table (13) of actions in the case where the checks associated with the requested transition are not satisfied (524).

27. A method according to any one of Claims 11 to 26, characterised in that the said method does not enable the crossover of a state transition, from an additive state to a reference state.

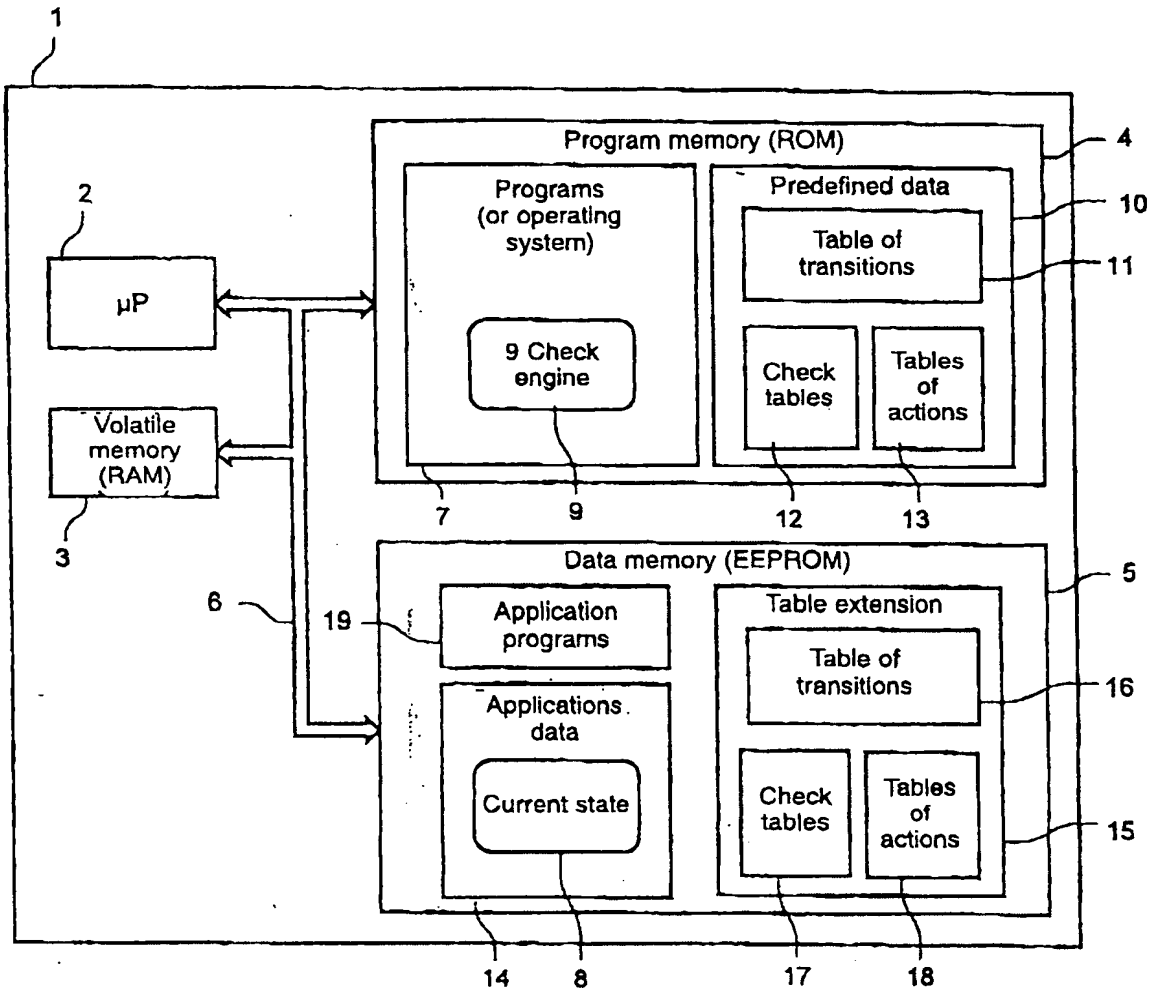

1
Program memory (ROM)
4
2
Programs
(or operating
system)
Predefined data
10
Table of
transitions
11
µP
9 Check
engine
Check
tables
Tables
of
actions
Volatile
memory
(RAM)
3
7
9
12
13
Data memory (EEPROM)
5
6
19
Application
programs
Table extension
Table of
transitions
16
Applications
data
Current state
Check
tables
Tables
of
actions
15
14
8
17
18

FIG. 1

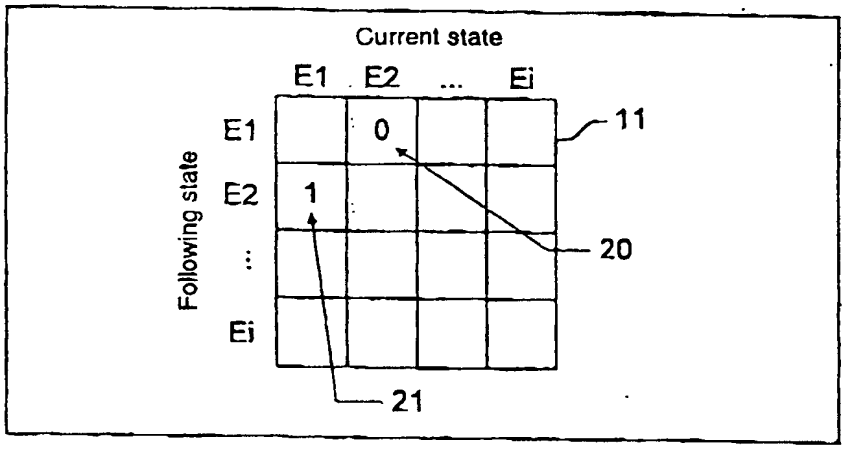

Current state
E1
E2
...
Ei
Following state
E1
E2
Ei
0
1
11
20
21

FIG. 2a

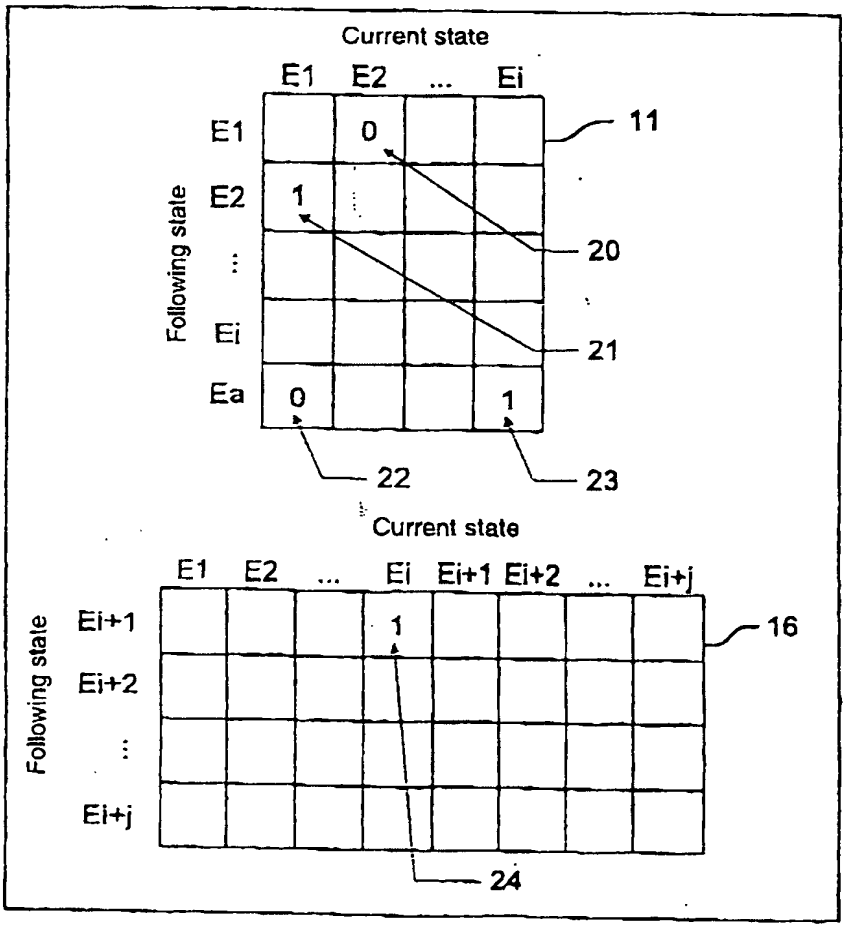

Current state
E1
E2
...
Ei
Following state
E1
E2
Ei
Ea
0
1
11
20
21
0
1
22
23
Current state
E1
E2
...
Ei
Ei+1
Ei+2
Ei+j
Following state
Ei+1
Ei+2
Ei+j
1
16
24

FIG. 2b

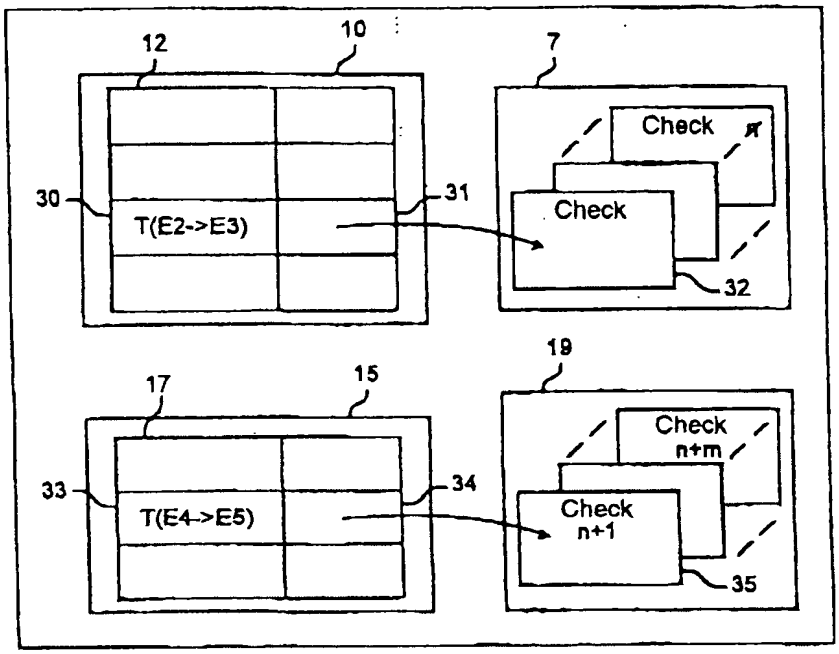

12
10
7
Check n
Check
30
T(E2->E3)
31
32
17
15
19
Check n+m
Check n+1
33
T(E4->E5)
34
35

FIG. 3

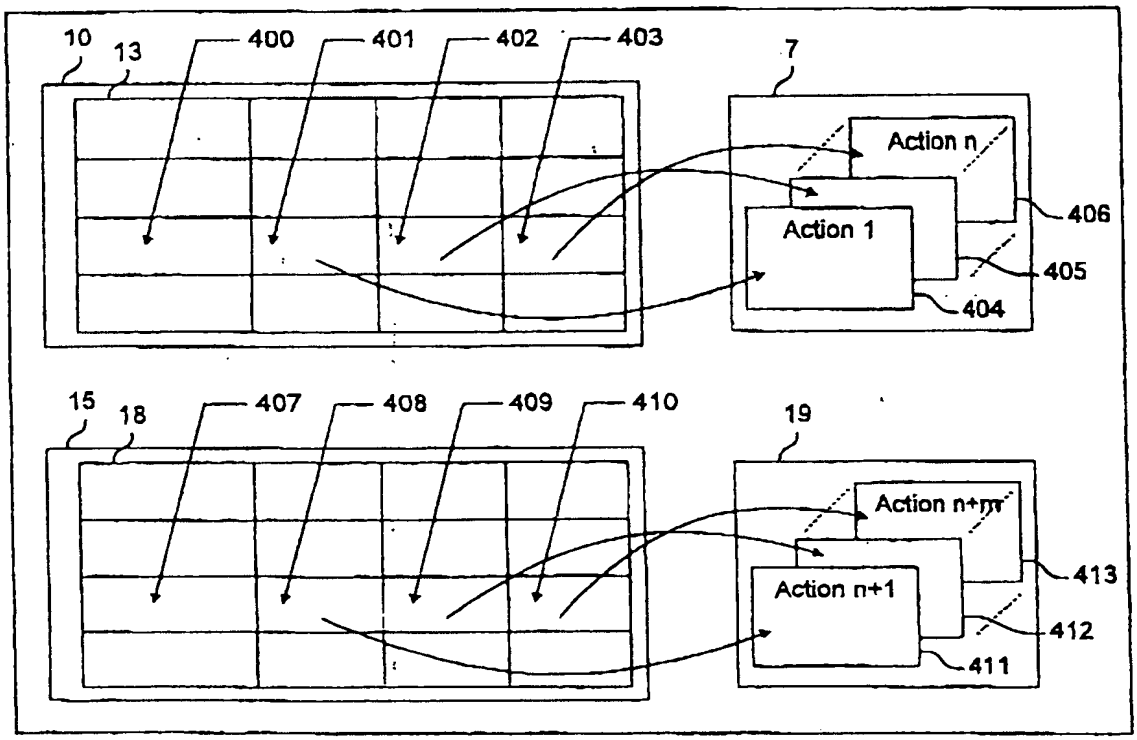

10
13
400
401
402
403
7
Action n
Action 1
406
405
404
15
18
407
408
409
410
19
Action n+m
Action n+1
413
412
411

FIG. 4

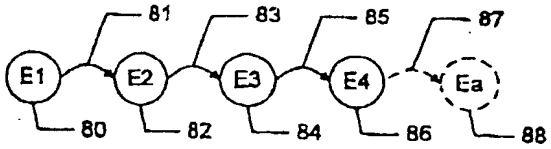


FIG. 6a

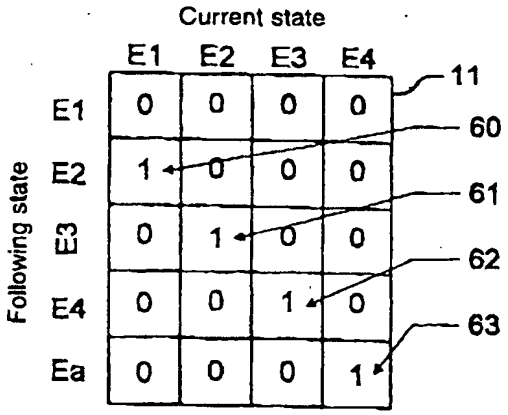


FIG. 6b

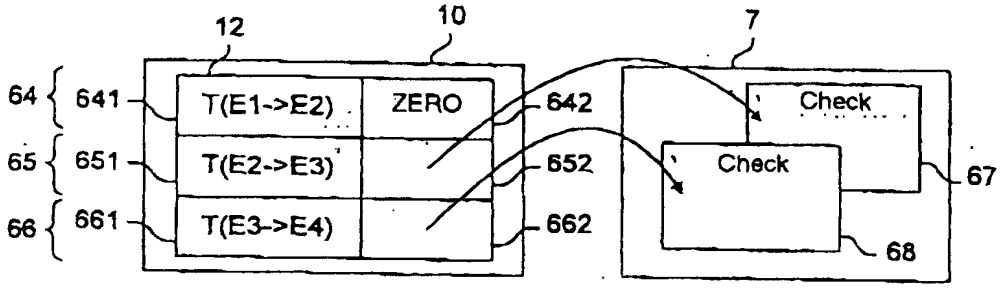


FIG. 6c

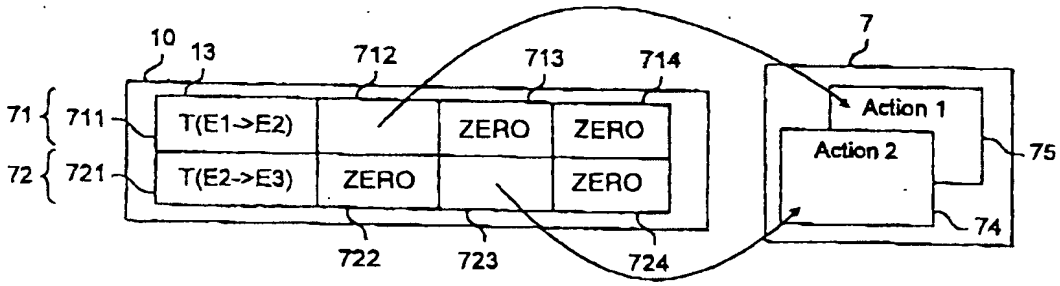


FIG. 6d

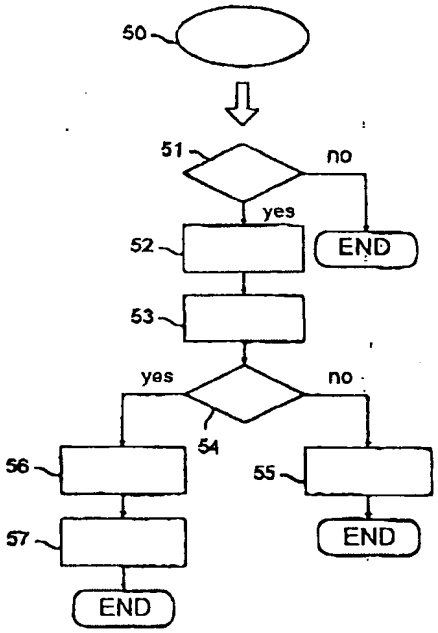


FIG. 5a

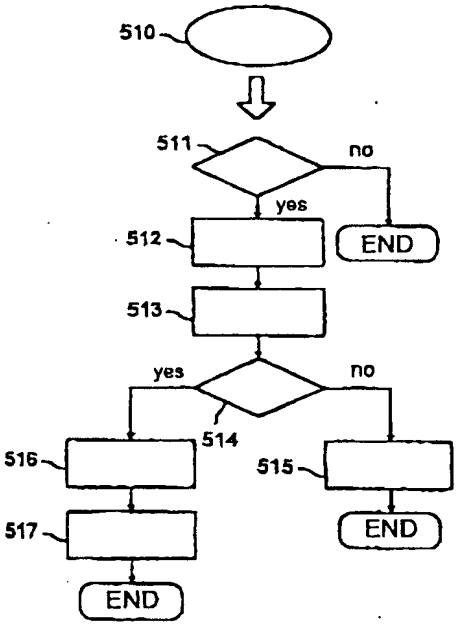


FIG. 5b

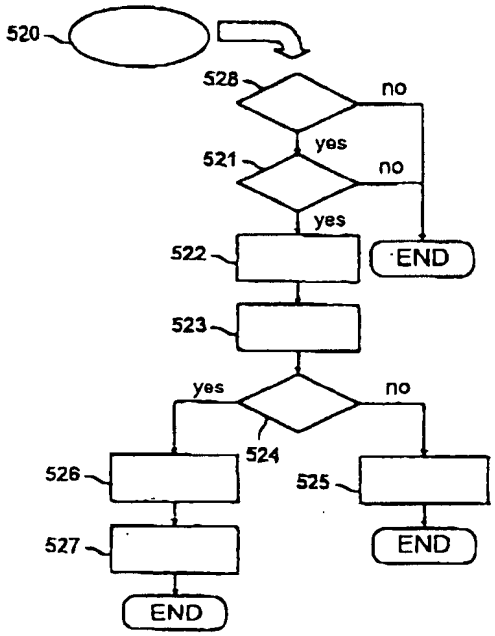


FIG. 5c

9

Translation 09/831745

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 555	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02678	International filing date (*day/month/year*) 03 November 1999 (03.11.99)	Priority date (*day/month/year*) 13 November 1998 (13.11.98)
International Patent Classification (IPC) or national classification and IPC G06K 19/073		
Applicant GEMPLUS		

RECEIVED
NOV 0 9 2001
Technology Center 2100

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 29 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 25 May 2000 (25.05.00)	Date of completion of this report 14 February 2001 (14.02.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/02678

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages _____, as originally filed
pages _____, filed with the demand
pages 1-19, filed with the letter of 20 December 2000 (20.12.2000)

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-36, filed with the letter of 20 December 2000 (20.12.2000)

☒ the drawings:

pages 1/5-5/5, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-36	YES
	Claims		NO
Inventive step (IS)	Claims	1-36	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-36	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following document:

D1: US-A-5473690

1. The invention concerns a device for controlling the life cycle of a portable electronic object, the life cycle being determined by a succession of states of transition, said states determining the services offered by the card. This invention also concerns a method for controlling the life cycle of a portable electronic object.

The closest prior art is D1, which describes a smart card that is capable of containing several distinct applications, for example, relating to a bank, garage, social security, etc... Access to each of its applications is protected by a different password (see Figure 3, and the corresponding description). The passing from one application to another corresponds to a state of transition of the card. Furthermore, the life cycle of the card is characterised by numerous transitions from one application to another, and, hence, from one state

of the card to another. Since the access to each application is protected by a password, it is implicit that the card comprises means of controlling the validity of passwords, hence, constituting a means for controlling the transition from one state to another. Furthermore, the card also comprises a processing unit (11; Figure 2), a volatile memory (registers of microprocessor 3), program memories (13), and data memories (12), each of these memories having a content defining a plurality of configurations.

The objective problem of D1 solved by the present invention can be considered to be that of providing an irreversible passage of the object from one state to another, in the course of the card life cycle, in particular for reasons of security.

The invention solves this problem by the fact that the control device comprises means for controlling the transition of the portable electronic object from a first to a second state, by using state transition authorisation and/or blocking means, such that only some transitions among all possible transitions are permitted.

No single cited document in the International Search Report suggests such a control of transition from one state to another. In D1, there is nothing to prevent passing from one application to another if the password is known.

International application No.
PCT/FR 99/02678

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The description is not in accordance with the claims, as required by PCT Rule 5.1(a)(iii), with respect to the definition of the invention on pages 5 to 7.

TRAITE DE COOPERATION EN MATIER E BREVETS

REPLACED BY ART 34 AMDT

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

15T

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 555	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02678	Date du dépot international *(jour/mois/année)* 03/11/1999	Date de priorité *(jour/mois/année)* 13/11/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06K19/073		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 29 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
25/05/2000	14.02.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Paci, M N° de téléphone +49 89 2399 2282

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02678

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

1-19	reçue(s) le	27/12/2000	avec la lettre du	20/12/2000

Revendications, N°:

1-36	reçue(s) le	27/12/2000	avec la lettre du	20/12/2000

Dessins, feuilles:

1/5-5/5	version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n^{os} :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-36
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-36
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-36
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

Conc rnant l p int V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventiv et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant:

D1: US-A-5473690

1. L'invention concerne un dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par la carte. L'invention concerne également un procédé de contrôle du cycle de vie d'un objet électronique portatif.

   L'état de la technique le plus proche est D1 qui décrit un carte à puce pouvant contenir plusieurs applications distinctes concernant par exemple une banque, un garage, la sécurité sociale, etc... L'accès à chacune de ces applications est protégé par un mot de passe différent (voir figure 3 et la description correspondante). Le passage d'une application à une autre correspond à une transition d'un état de la carte à un autre état de la carte. De plus, le cycle de vie de la carte est caractérisé par de nombreux passages d'une application à une autre, et donc d'un état de la carte à un autre. Etant donné que l'accès à chaque application est protégé par un mot de passe, il est implicite que la carte comporte des moyens de contrôle de la validité des mots de passe constituant donc un dispositif de contrôle de la transition d'un état à un autre. De plus, la carte comprend également une unité de traitement (11; figure 2), une mémoire volatile (les registres du microprocesseur 3), des mémoires de programme (13) et des mémoires de données (12), chacune de ces mémoires présentant un contenu définissant une pluralité de configurations.

   Le problème objectif de D1 résolu par la présente invention est permettre un passage irréversible d'un état à un autre état de l'objet au cours du cycle de vie de la carte, notamment pour des raisons de sécurité.

L'invention résout ce problème en ce que le dispositif de contrôle comporte des moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif, exploitant des moyens d'autorisation et/ou interdiction de transition d'état, de sorte que seules certains transitions ne soient permises parmi l'ensemble des transitions possibles.

Aucun des documents cités dans le rapport de recherche international ne suggère un tel contrôle du passage d'un état à un autre. Dans D1, rien n'empêche de passer d'une application à une autre si l'on connaît le mot de passe.

Concernant le point VII
Irrégularités dans la demande internationale

La description ne concorde pas avec les revendications, comme l'exige la règle 5.1 a) iii) PCT, en ce qui concerne la définition de l'invention aux pages 5 à 7.

PROCEDE ET DISPOSITIF DE CONTROLE DU CYCLE DE VIE D'UN OBJET PORTATIF, NOTAMMENT D'UNE CARTE A PUCE

L'invention concerne les objets électroniques portatifs tels que les cartes à microcircuits électroniques, dites cartes à puce qui, connectées à des dispositifs électroniques pour permettre à ces derniers de réaliser des fonctions particulières dans le cadre d'une ou plusieurs applications, nécessitent un contrôle de leurs étapes de vie. Lesdites cartes sont en effet généralement utilisées dans des applications (banque, communication, identité, santé...) nécessitant une grande sécurité contre les usages frauduleux. Ainsi, à titre d'exemple, le document US 5473690 présente une carte à puce comprenant plusieurs applications dont l'accès est protégé par mots de passe, un mot de passe étant dédié à un utilisateur. Connaissant un mot de passe, il est possible de sélectionner telle ou telle application. Cependant, on ne peut désactiver une application ou en limiter l'usage quel que soit l'utilisateur de la carte en fonction des étapes de vie de ladite carte.

L'invention s'applique plus généralement à tout système embarqué indépendant, doté d'une unité de traitement et des mémoires de programme et de données.

Il est connu dans le monde de la carte à puce que celle-ci résulte d'un assemblage d'un composant (comprenant en général un microprocesseur en relation avec des mémoires via des bus de communication), d'un module (réalisé à l'aide d'un métal conducteur) auquel est relié ledit composant (dans le cadre d'une carte à puce dite à contact) pour permettre audit composant d'être connecté à un dispositif électronique de lecture et/ou écriture (ou coupleur) et d'un corps de carte ou plus généralement d'un support sur lequel est intégré l'ensemble module/composant.

Dans la cadre d'une carte à puce dite sans contact, ledit module est remplacé par une antenne et l'ensemble formé par le composant et ladite antenne est intégrée au sein dudit support.

La vie d'une carte à puce se décompose généralement en deux ensembles d'étapes se succédant les unes aux autres, correspondant respectivement à la fabrication et à l'exploitation de ladite carte. La composition des deux ensembles d'étapes forme un cycle de vie de ladite carte. La fabrication d'une carte à puce (à contact ou sans contact) est constituée de plusieurs étapes.

En effet, il est tout d'abord nécessaire de disposer d'un composant électronique qui est initialisé, isolé, puis relié à un module. Ledit composant et le module, auquel il est relié, sont par la suite intégrés sur ou au sein d'un support (généralement un corps de carte plastique) lui même imprimé à des fins d'identification ou de publicité. Par la suite la carte à puce ainsi obtenue est initialisée ou programmée pour répondre aux conditions d'utilisation dans le cadre d'applications.

Le second ensemble d'étapes de vie d'une carte à puce correspond à son exploitation. Cet ensemble peut lui-même être divisé en plusieurs étapes, chacune correspondant, par exemple, à l'implantation ou la suppression de services offerts par la carte à puce à l'utilisateur en fonction de son profil par exemple.

En outre différents acteurs (fabricant de composant, fabricant de cartes à puce, centre de personnalisation de cartes, émetteur de cartes, ou encore porteur de cartes) interviennent durant les différentes étapes de la fabrication et de l'exploitation d'une carte à puce. Ainsi, les composants sont fournis et parfois en partie initialisés par des fabricants de composants électroniques sur une tranche de silicium. Cette phase correspond à l'étape de fabrication du composant. L'étape suivante est

la phase d'encartage réalisée par le fabricant de carte à puce. Elle inclut l'isolement d'un composant de la tranche de silicium, la connexion dudit composant à un module (ou antenne), l'intégration de l'ensemble sur leur support ou corps de carte. Suit la préparation de la structure applicative présente dans la mémoire programmable électriquement du composant. C'est l'étape de personnalisation électrique qui est réalisée par le fabricant des cartes à puce ou par un centre de personnalisation ou un tiers spécialisé dans la personnalisation des cartes ou par l'émetteur lui-même qui est chargé in fine de la distribution des cartes sur le marché. Cette phase de personnalisation électrique peut donc être décomposée en autant d'étapes qu'il y a d'acteurs ou d'intermédiaires. Par la suite, durant l'exploitation de la carte à puce, nous avons vu précédemment qu'il peut être intéressant de distinguer différentes étapes au gré de l'évolution du profil de l'utilisateur de la carte par exemple. Pour toutes ces raisons, il est donc important de suivre rigoureusement les étapes de vie d'une carte pour connaître à tout moment l'étape en-cours de ladite carte au sein de son cycle de vie. De plus, il est indispensable que, d'une part, l'accès en écriture ou en lecture de la mémoire programmable électriquement du composant d'une carte soit protégé durant l'échange de ladite carte (ou du composant) entre les différents acteurs et que d'autre part l'accès à ladite mémoire soit limité au fur et à mesure que se succèdent les étapes de vie de la carte citées précédemment, en activant ou désactivant des services par exemple. Pour finir, il est également nécessaire parfois de valider le contexte applicatif de la carte à puce avant que le porteur de celle-ci l'utilise sur le marché. Par exemple, un émetteur de carte à puce de type porte-monnaie électronique, doit être certain que la balance de ladite carte est bien nulle avant d'émettre la carte.

Pour tenter de répondre à ces exigences, différentes solutions sont utilisées à ce jour. Certaines solutions sont purement extérieures à la carte à puce (sécurisation physique des locaux où ladite carte est fabriquée, utilisation de moyens de transport eux-mêmes sécurisés...). D'autres solutions complémentaires aux premières, mais cette fois internes ou implantées dans la carte, sont aussi généralement utilisées. On utilise ainsi des secrets permettant de protéger l'accès en lecture/écriture de la mémoire du composant et également des indicateurs logiques permettant de suivre de manière irréversible les différentes étapes de vie de la carte. Pour cela, des bits au sein d'une mémoire non effaçable du composant de la carte à puce sont positionnés à l'état actif à la fin des différentes étapes de vie de la carte (fabrication et initialisation du composant par le fabricant dudit composant, encartage et initialisation de la mémoire de la carte par le fabricant de carte à puce, préparation de la structure applicative de la mémoire de la carte à puce par le centre de personnalisation ou l'émetteur de la carte...). En fonction de ces indicateurs, le programme (ou système d'exploitation), exécuté par le microprocesseur du composant de la carte à puce, implanté au sein de l'une des mémoires dudit composant de ladite carte, adapte son comportement au fur et à mesure que les étapes de vie de ladite carte se succèdent. Ainsi, des fonctions peuvent être modifiées, ajoutées ou supprimées.

Quelles que soient les solutions utilisées à ce jour, elles reposent toutes sur le fait que les différents acteurs impliqués dans la fabrication d'une carte sont des tiers de confiance. Seules des personnes, susceptibles d'intercepter des composants ou des cartes durant leur transfert entre deux des différents acteurs, sont supposées

"fraudeurs potentiels" et les solutions exposées précédemment permettent de s'en affranchir. L'adaptation du système d'exploitation de la carte en fonction des indicateurs irréversibles apporte un plus non négligeable. Ainsi, si les fabricants de composants ou de cartes inscrivent des données systèmes ou des secrets, l'émetteur de la carte ne pourra par exemple librement s'affranchir desdits secrets ou modifier lesdites données système. Cependant, cette solution ne résout pas le problème d'une initialisation frauduleuse de la carte ou d'une erreur malencontreuse durant ladite initialisation, effectuée par l'un des acteurs.

L'invention propose de remédier aux inconvénients de l'état actuel de la technique. En particulier, l'invention consiste à doter le système d'exploitation d'une carte à puce de moyens logiciels permettant audit système d'exploitation de maîtriser un changement irréversible d'étape de vie de ladite carte en fonction d'un ensemble de vérifications du contenu des mémoires de cette même carte à puce. En outre l'invention prévoit que lors d'un changement d'étape de vie, le système d'exploitation de la carte puisse déclencher automatiquement des actions permettant d'adapter les services offerts par ledit système d'exploitation de ladite carte.

A cet effet, l'invention concerne un dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant constitué par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, chacune de ces mémoires présentant un contenu définissant une pluralité de configurations, caractérisé en ce qu'il comporte des

moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif.

Selon d'autres caractéristiques du dispositif selon l'invention :

- les moyens de contrôle comportent :
  - des moyens d'autorisation et/ou d'interdiction de transition d'états à effectuer;
  - des moyens de vérification du contenu de la mémoire volatile, des mémoires de données et des mémoires de programme de l'objet électronique portatif en fonction de la transition d'états à effectuer;
  - des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement d'une transition d'état.

En outre, l'invention concerne un objet électronique portatif, pouvant être notamment une carte à puce, comportant ledit dispositif de contrôle du cycle de vie.

Par ailleurs, l'invention concerne un procédé de contrôle du cycle de vie d'un objet électronique portatif, ledit procédé étant mis en œuvre au sein de l'objet à la suite d'une demande de transition d'états,

caractérisé en qu'il comprend :

- une étape de validation de l'autorisation de ladite demande;
- une étape d'évaluation des vérifications associée à la transition demandée;
- une étape de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée et, si les vérifications de la configuration de l'objet sont satisfaites.

Selon d'autres caractéristiques, le procédé comprend éventuellement en outre :

- une étape d'exécution d'actions systématiques;
- une étape d'exécution d'actions positives dans le cas où la transition demandée est autorisée et si les vérifications associées à la transition demandée sont satisfaites;
- une étape d'exécution d'actions négatives dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre indicatif et nullement limitatif de l'invention.

Les figures montrent:

- figure 1: un composant d'une carte à puce munie d'un dispositif de vérification de transition d'état;
- figures 2a et 2b: une représentation détaillée d'une table des transitions d'état;
- figure 3: une représentation détaillée d'une table des vérifications des transitions;
- figure 4: une représentation détaillée d'une table des actions;
- figure 5: une description des étapes mises en ouvre dans le procédé utilisé par le dispositif de vérification de transitions;
- figures 6a à 6d: les particularités mises en œuvre dans le cas d'un exemple d'une carte à puce de type porte-monnaie électronique.

Dans l'invention, on appellera état de référence, un état à partir duquel il est possible de basculer vers un autre état suite au franchissement d'une transition décrite dans la table des transitions, implantée dans la mémoire de

programme. Comme il est décrit plus loin, il est possible d'ajouter de nouveaux états et donc de nouvelles transitions après que l'étape de fabrication du composant ait eu lieu. Dans ce cas, on parlera d'états additifs pour caractériser ceux-ci par opposition aux états de référence. D'autre part, on appellera état courant l'état dans lequel se trouve le système embarqué.

La figure 1 montre un composant 1, d'une carte à puce, muni d'un dispositif de vérification de transitions selon l'invention. Le composant comporte une unité de traitement 2 ou encore microprocesseur en relation avec des mémoires 3, 4 et 5 via un bus de communication 6. Une mémoire de programme 4 (ou encore ROM) non effaçable comporte d'une part une zone de programmes 7, lesdits programmes (ou encore système d'exploitation du système embarqué) pouvant être exécutés par ladite unité de traitement et d'autre part une zone de données prédéfinies 10 qui contient des constantes utilisées par ledit système d'exploitation. Parmi lesdites constantes de la zone 10, le système d'exploitation 7, comportant un programme appelé moteur de vérification 9, exploite une table des transitions 11 qui permet de préciser les états auxquels on peut accéder à partir de l'état courant, une table des vérifications 12 qui permet d'associer à chaque transition d'état des vérifications portant sur le contenu des mémoires 3, 4 et/ou 5. Dans une variante, le moteur de vérification 9 peut déclencher automatiquement des actions lors du franchissement ou du rejet du franchissement d'une transition. Pour cela la zone 10 de la mémoire de programme comporte une table des actions 13 qui permet d'associer à chaque transition d'état possible des actions à effectuer.

Une mémoire volatile 3 (ou encore RAM pour Random Access Memory en langue anglaise) permet à l'unité de traitement 2 de stocker de manière temporaire des résultats

ou encore des secrets issus de calculs décrits par les programmes implantés dans la mémoire de programme 4. Le contenu de la mémoire 3 est effacé à chaque mise sous tension du composant 1 ou à chaque demande de remise à zéro de celui-ci.

Une mémoire de données 5, effaçable électriquement utilisant généralement la technologie EEPROM (pour Electrical Erasable Programmable Read Only Memory en langue anglaise) comporte une zone 14 contenant les données variables nécessaires à l'exécution des programmes 7. Cette zone 14 comporte notamment une donnée 8 appelée "Etat courant" permettant de mémoriser l'état courant de l'objet électronique portatif. La mémoire de données 5 comporte en outre une zone 15 comprenant optionnellement des extensions des tables 11 à 13 dans le cas où il est nécessaire d'ajouter des états aux états de références. La zone 15 comporte alors une extension de la table des transitions 16, une extension de la table des vérifications 17 et peut comporter une extension de la table des actions 18 si l'on souhaite associer aux nouvelles transitions d'état additif des actions, comme vu précédemment pour ce qui concerne la table 13. Dans le cas d'ajout d'états par rapport aux états de référence, il est parfois indispensable d'enrichir le système d'exploitation 7. Pour cela, la mémoire 5 peut comporter en outre une zone 19 qui contient les programmes supplémentaires qui seront exécutés à leur tour par l'unité de traitement 2.

La figure 2a montre une mise en oeuvre possible de la table des transitions 11. Si l'on suppose que l'on dénombre i états de référence, on peut imaginer une table de transition comprenant i colonnes et i lignes. Les colonnes correspondent aux états de référence pouvant être, à un instant donné, l'état courant. Les i premières lignes correspondent aux états de référence auxquels on peut

accéder à partir de l'état courant. Ainsi la valeur d'une case de la table des transitions 11 correspondant à l'intersection d'une ligne et d'une colonne de ladite table permet de coder soit, l'absence de transition autorisée (valeur nulle par exemple - c'est le cas de la transition 20), soit, l'autorisation une transition (valeur non nulle - c'est le cas de la transition 21). Dans le cas d'une transition autorisée, le moteur de vérification de transitions recherche au sein de la table de vérification 12 les vérifications à effectuer pour accepter ou rejeter le franchissement de la transition demandée.

La figure 2b montre également une mise en oeuvre possible d'une table de transition dans le cas où il est possible d'ajouter des états (états additifs) aux états de référence. La table des transitions comporte une ligne supplémentaire par rapport à la figure 2a. La (i+1)ème ligne permet de préciser si l'on autorise des transitions d'un état de référence courant à un état additif. Ainsi la valeur de la case 22 indique une transition interdite d'un état de référence vers un état additif. La case 23 indique qu'il sera possible de basculer de l'état de référence Ei vers un état additif. Une extension 16 de la table des transitions est alors nécessaire. Cette dernière comporte j lignes correspondant à j états additifs auxquels on peut accéder à partir de (i+j) états courant possibles matérialisés par les (i+j) colonnes de l'extension 16 de la table des transitions. Ainsi la combinaison de la case 23 de la table des transitions et de la case 24 de l'extension 16 de la table des transitions, indique au moteur de vérification qu'il est possible de basculer de l'état de référence Ei vers l'état additif E(i+1).

La figure 3 montre une mise en oeuvre de la table des vérifications. La table des vérifications 12 est implantée

au sein de la zone 10 des données prédéfinies de la mémoire 4. Chaque transition autorisée dispose d'une entrée dans ladite table. Une entrée comprend un champ 30 permettant d'identifier la transition et un champ 31 contenant une référence (ou adresse) vers un programme 32 du système d'exploitation 7. Le moteur de vérification 9 peut ainsi faire exécuter à l'unité de traitement 2 les contrôles requis pour accepter le franchissement de la transition. La figure 3 illustre également une structure d'une extension 17 de la table des vérifications. De la même manière que pour la table 12, l'extension de la table des vérifications 17 comporte une entrée par transition possible. Chaque entrée comprend deux champs, un champ 33 permettant d'identifier la transition et un champ 34 contenant une référence (ou adresse) d'un programme 35 du système d'exploitation ou, comme le montre la figure 3, d'un programme supplémentaire implanté dans la mémoire de données 5 (en zone 19).

La figure 4 montre une représentation de la table des actions 13 implantée dans la zone 10 des données prédéfinies de la mémoire de programmes 4. Lors d'une demande de franchissement de transition, il est possible de déclencher des actions. Celles-ci peuvent être de trois types: action systématique, action positive (c'est à dire conditionnée au fait que les vérifications sont satisfaisantes) ou action négative (c'est à dire conditionnée au fait que les vérifications ne sont pas satisfaisantes). La figure 4 montre qu'à chaque transition autorisée, il existe une entrée dans la table des actions 13. Cette entrée comprend 4 champs. Le premier champ 400 permet d'identifier la transition. Les trois autres champs 401, 402 et 403 contiennent chacun une référence ou adresse d'un programme 404, 405 ou 406 du système d'exploitation. Le champ 401 est dédié à une action systématique, le champ

402 à une action positive et le champ 403 à une action négative. La figure 4 montre également une extension 18 de la table des actions. Cette table 18 est implantée dans la zone 15 de la mémoire de données 5 du composant 1. De la même manière que pour la table des actions 13, l'extension de la table des actions 18 comprend une entrée par transition possible. Une entrée comprend 4 champs. Le premier champ 407 permet d'identifier la transition. Les trois autres champs 408, 409 et 410 contiennent chacun une référence ou adresse d'un programme 411, 412 ou 413 du système d'exploitation ou comme le montre la figure 4, des programmes implantés dans la zone 19 de la mémoire de données 5 du composant 1. Le champ 408 est dédié à une action systématique, le champ 409 à une action positive et le champ 410 à une action négative.

La figure 5a décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état de référence vers un autre état de référence. La demande de franchissement d'une transition peut être formulée suite à un ordre du fabricant de carte ou par tout autre acteur du cycle de vie de la carte à puce. Ladite demande peut également être formulée directement par la carte-elle même, par exemple au travers d'une action associée à une transition. Dans le cadre de la figure 5a, l'état de référence courant est l'état Ei. L'ordre 50 de basculement de l'état Ei à l'état Ej est formulé. L'étape 51 consiste à vérifier au sein de la table des transitions 11 que la transition de l'état Ei vers l'état Ej est autorisée. Dans le cas où cette transition est interdite, la demande de franchissement de transition 50 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela le moteur de vérification évalue l'entrée de la

table des vérifications 12 dédiée à la transition T(Ei->Ej). L'exécution desdites vérifications correspond à l'étape 52 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de la table des actions 13 dédiées à ladite transition (étape 53). Si les vérifications 54 exigées lors de la demande de franchissement de la transition 50 sont non satisfaisantes, l'état courant demeure inchangé. En fonction de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej) le moteur de vérifications exécute les actions négatives (étape 55 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 54 sont satisfaisantes, alors l'état courant devient l'état Ej (étape 56 du procédé). Les actions positives sont alors exécutées (étape 57 du procédé) en fonction de l'état de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5b décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état additif vers un autre état additif. L'état additif courant est l'état Ei. L'ordre 510 de basculer de l'état additif Ei à l'état additif (ou de référence) Ej est formulé. L'étape 511 du procédé consiste à vérifier au sein de l'extension la table des transitions 16 que la transition de l'état Ei à l'état Ej est autorisée. Dans le cas où cette transition est interdite, la demande de franchissement de transition 510 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela, le moteur de vérification évalue l'entrée de l'extension de la table des vérifications 17 dédiée à la transition T(Ei-

>Ej). L'exécution desdites vérifications constitue l'étape 512 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de l'extension de la table des actions 18 dédiées à ladite transition (étape 513 du procédé). Si la vérification 514 exigée lors de la demande de franchissement de la transition 510 est non satisfaisante, l'état courant demeure inchangé. En fonction de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej), le moteur de vérification 9 exécute les actions négatives (étape 515 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 514 sont satisfaisantes, l'état courant devient l'état Ej (étape 516 du procédé). Les actions positives sont alors exécutées (étape 517 du procédé) en fonction de l'état de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5c décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un état de référence vers un état additif. L'état de référence courant est l'état Ei. L'ordre 520 de basculement de l'état de référence Ei à l'état additif Ej est formulé. L'étape 528 du procédé consiste à vérifier au sein de la table des transitions 11, qu'une transition de l'état de référence courant Ei vers un état additif est autorisée. Si une telle transition est interdite, le procédé est terminé. L'état courant demeure inchangé. Par contre, si une transition dudit état de référence vers un état additif est autorisée, le moteur de vérification déroule les étapes 521 à 527 du procédé, respectivement identiques aux étapes 511 à 517 décrites en liaison avec la figure 5b.

Un exemple d'application dans le domaine du Porte-monnaie électronique est présenté en liaison avec les figures 6a à 6d. Ladite application permet de régler des achats à l'aide "d'argent électronique" stocké dans une carte à puce, au lieu de payer en numéraire. L'emploi d'une telle technique impose une gestion des cartes aussi sécurisée que celle qu'aurait imposé l'emploi du numéraire. Il faut par exemple éviter la création de monnaie fictive. La sécurité d'une carte à puce porte-monnaie électronique repose généralement sur des clés stockées à l'intérieur de ladite carte à puce permettant des transactions sécurisées en utilisant la cryptographie. Une telle carte dispose d'un système d'exploitation offrant un jeu de commandes et de services permettant de créditer ou de débiter de l'argent. Au début du cycle de vie de la carte à puce porte-monnaie électronique, ladite carte à puce n'est pas initialisée. Elle ne contient aucune information. La figure 6a montre les états de référence prédéfinis :

- Etat E1 "carte vierge" (référencé 80): seules des commandes de test permettant de valider le comportement de la mémoire de données 5 sont disponibles (vérification que les cases mémoires de technologie EEPROM peuvent être correctement écrites et effacées);

- Etat E2 "carte testée" (référencé 82): Les commandes de test ne sont plus disponibles. A leur tour des commandes dites généralement "commandes physiques" (permettant un accès en écriture par un adressage physique indépendamment de toute structure logique de type fichier par exemple) sont disponibles. Elles permettent d'initialiser la carte (écriture dans la zone 14 de la mémoire de données des constituants logiques nécessaires au fonctionnement de l'application c'est à dire fichiers, balances...);

- Etat E3 "carte initialisée" (référencé 84): les commandes physiques ne sont plus disponibles. Des commandes logiques permettent de personnaliser la carte (ajout de

nouvelles structures logiques et initialisation de données dans lesdites structures) sont utilisables. En outre, un mécanisme de recouvrement est activé de sorte que la carte à puce ne perde pas la cohérence de ces données lors d'une mise hors tension de celle-ci durant l'exécution de l'une desdites commandes logiques.

- Etat E4 "carte personnalisée" (référencé 86): les commandes logiques spécifiques à l'application Porte-monnaie électronique (débit/crédit) sont activées.

Le jeu de commandes disponibles évolue en fonction de l'étape de vie dans laquelle se trouve la carte à puce. Des informations stockées en mémoire de données permettent au système d'exploitation de connaître l'état dans lequel la carte à puce se trouve. La figure 6a montre en outre que dans le cadre d'une carte de type porte-monnaie électronique, toutes les transitions entre états de référence doivent être franchies successivement (de l'état E1 à l'état E4) et ce de manière irréversible. Toute autre transition est interdite. Seule la possibilité d'utiliser ultérieurement des états additifs 88 est offerte. Cette transition possible est référencée 87. Le système d'exploitation en fonction de l'état courant n'autorise qu'un ensemble de commandes spécifiques à chaque état de référence.

Les vérifications et les actions à déclencher lors du franchissement d'une transition sont décrites comme suit :

- Transition de l'état E1 vers l'état E2 (notée T(E1->E2) et référencée 81) :
  - Vérification: aucune
  - Action systématique :
    effacement de la mémoire de données pour éviter qu'un fraudeur y laisse des données interprétables par le système d'exploitation de la carte;

- Transition de l'état E2 vers l'état E3 (notée T(E2->E3) et référencée 83) :
  - Vérification:
    - intégrité des données écrites dans la mémoire de données avec les commandes physiques (validation d'un code de redondance par donnée);
    - vérification de l'état vierge de la mémoire en dehors desdites données;
  - Action positive :
    - activation du mécanisme de recouvrement;
- Transition de l'état E3 vers l'état E4 (notée T(E3->E4) et référencée 85) :
  - Vérification:
    - nullité de la balance du porte monnaie électronique
  - Action : aucune
- Transition de l'état E4 vers un état additif (notée T(E4->Eadd) et référencée 87) :
  - Vérification : aucune
  - Action : aucune

Les figures 6b à 6d illustrent respectivement une réalisation d'une table des transitions 11, d'une table des vérifications 12 et d'une table d'actions 13, selon l'invention. La table des transitions 11 telle que décrite en liaison avec la figure 6b permet de n'autoriser que les transitions 81, 83, 85 et 87. Pour cela seules les cases 60 à 63 de ladite table contiennent une valeur non nulle. Les autres cases de la table des transitions contiennent une valeur nulle pour indiquer que toute autre transition est interdite. La table des vérifications telle que présentée au travers de la figure 6c, permet d'associer les vérifications à satisfaire pour autoriser le franchissement des transitions 81, 83, 85 et 87, lesdites transitions

autorisées par la table des transitions 11 (figure 6b). Ainsi l'entrée 64 de la table des vérifications 12 comporte un champ 641 permettant d'identifier que ladite entrée est dédiée à la transition 81. L'entrée 64 comporte en outre un champ 642 contenant une référence nulle pour indiquer qu'aucune vérification n'est demandée pour autoriser le franchissement de la transition 81. Dans une variante, la transition 81 ne dispose d'aucune entrée associée. Cette variante est illustrée plus loin dans le cas de la table des actions. La table des vérifications 12 comporte une entrée 65 qui comprend respectivement un champ 651 pour indiquer que l'entrée est associée à la transition 83 et un champ 652 contenant la référence d'un programme 67, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment. De même, la table des vérifications 12 comporte une entrée 66 qui comprend respectivement un champ 661 pour indiquer que l'entrée est associée à la transition 83 et un champ 662 contenant la référence d'un programme 68, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment.

La figure 6d présente une réalisation de la table des actions 13. Ladite table comporte une entrée 71 qui comporte un champ 711 permettant d'indiquer que ladite entrée est associée à la transition 81. La même entrée 71 comporte un champ 712 contenant la référence d'un programme 75, implanté dans la mémoire de programmes, afin que le moteur de vérification puisse exécuter les actions systématiques associées à la transition 81. L'entrée 71 comporte en outre un champ 713 et un champ 714 contenant une référence nulle pour indiquer au moteur de vérification qu'aucune action positive ni négative n'est associée au franchissement de la transition 81. De la même manière, la

table des actions 13 comporte une seconde entrée 72 comprenant les champs 721 à 724 pour indiquer au moteur de vérification que ladite entrée est associée à la transition 83, que le programme 74 est à exécuter comme action positive lors du franchissement de ladite transition et qu'aucune action systématique ou négative n'est à exécuter. L'absence d'entrée, au sein de la table des actions 13, associée à la transition 85, indique qu'aucune action (systématique, positive ou négative) n'est à exécuter lors du franchissement ou du rejet du franchissement de ladite transition.

Grâce au dispositif et au procédé tels que décrits ci-dessus, le cycle de vie d'un objet électronique portatif est maîtrisé. Chaque transition d'états est irréversible et les vérifications faites lors de chaque demande de transitions garantissent une configuration mémoire de l'objet cohérente. En outre les actions systématiques, positives ou négatives permettent d'adapter le comportement dudit objet. Enfin, dans le cas où il est prévu d'autoriser une ou plusieurs transitions d'un ou plusieurs états de référence vers un état additif, le cycle de vie de l'objet peut être facilement enrichi, par exemple après que l'objet soit émis sur le marché, sans que le cycle de vie prédéfini (composé par une succession de transitions d'état de référence vers un autre état de référence) puisse être détourné.

Tout risque de fraude durant l'initialisation d'un objet électronique portatif ou d'erreur malencontreuse durant ladite initialisation est écarté tout en conservant grande adaptabilité du contrôle du cycle de vie de l'objet.

REVENDICATIONS

1. Dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif, exploitant des moyens d'autorisation et/ou interdiction de transitions d'état, de sorte que seules certaines transitions ne soient permises parmi l'ensemble des transitions possibles.

2. Dispositif selon la revendication 1, caractérisé en ce que les moyens de contrôle comprennent des moyens de vérification du contenu de la mémoire volatile (3), des mémoires de données (5) et des mémoires de programmes (4) de l'objet électronique portatif, en fonction de la transition d'états permise à effectuer.

3. Dispositif selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que les moyens de contrôle autorisent et/ou interdisent une transition d'état en exploitant une table (11) des transitions d'état permises.

4. Dispositif selon la revendication 3, caractérisé en ce que les moyens de contrôle comprennent:

- outre la table (11) des transitions d'état permises;
- une table (12) des vérifications à effectuer par transition d'état permise;
- et un moteur de vérification (9) exploitant lesdites tables.

5. Dispositif selon la revendication 3, caractérisé en ce que les moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif comprennent:

- une extension (16) de la table (11) des transitions d'état permises;

6. Dispositif selon la revendication 4, caractérisé en ce que les moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif comprennent:

- une extension (16) de la table (11) des transitions d'état permises;
- une extension (17) de la table (12) des vérifications à effectuer par transition d'état permise;

et en ce que le moteur de vérification (9) exploite lesdites extensions de tables (16, 17).

7. Dispositif selon l'une quelconque des revendications 1 à 6, caractérisé en ce que les moyens de contrôle comprennent des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif.

8. Dispositif selon la revendication 7 lorsque celle-ci dépend des revendications 5 ou 6, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent une table (13) d'actions exploitable par le moteur de vérification (9).

9. Dispositif selon la revendication 8, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent une extension (18) de la table (13) d'actions exploitable par le moteur de vérification (9).

10. Objet électronique portatif, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'il comporte le dispositif de contrôle du cycle de vie de l'objet, selon l'une des revendications 1 à 9.

11. Carte à puce, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'elle comporte le dispositif de contrôle du cycle de vie de la carte, selon l'une des revendications 1 à 9.

12. Procédé de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

ledit procédé étant mis en œuvre, au sein de l'objet, à la suite d'une demande de transition d'états,

caractérisé en qu'il comprend :

- une étape (51, 511, 528, 521) de validation de l'autorisation de ladite demande en exploitant des moyens d'autorisation et/ou interdiction de transitions d'état, de sorte que seules certaines transitions ne soient permises parmi l'ensemble des transitions possibles;

- une étape (57, 517, 527) de modification de l'état courant de l'objet si la transition demandée est autorisée (51, 511, 528, 521).

13. Procédé selon la revendication 12, caractérisé en ce qu'il comprend une étape (53, 513, 523) d'exécution d'actions systématiques, actions associées à la transition demandée.

14. Procédé selon l'une quelconque des revendications 12 ou 13, caractérisé en ce qu'il comprend :

- une étape (52, 512, 522) d'évaluation des vérifications de la configuration de l'objet, vérifications associées à une transition permise;

- et en ce que l'étape (57, 517, 527) de modification de l'état courant de l'objet, est réalisée si lesdites vérifications de la configuration de l'objet sont satisfaites (54, 514, 524).

15. Procédé selon la revendication 14, caractérisé en ce qu'il comprend une étape (56, 516, 526) d'exécution d'actions positives, réalisée si la transition demandée est permise (51, 511, 528, 521), et si les vérifications associées à la transition demandée sont satisfaites (54, 514, 524).

16. Procédé selon l'une quelconque des revendications 14 ou 15, caractérisé en ce qu'il comprend une étape (55, 515, 525) d'exécution d'actions négatives si les vérifications associées à la transition demandée ne sont pas satisfaites (54, 514, 524).

17. Procédé selon l'une quelconque des revendications 12 à 13, caractérisé en ce qu'il comprend une étape (56, 516, 526) d'exécution d'actions positives réalisée si la transition demandée est permise (51, 511, 528, 521).

18. Procédé selon l'une quelconque des revendications 12 à 17, mis en œuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état de référence vers un second état de référence, caractérisé en que l'étape (51) de validation de l'autorisation de ladite demande consiste à analyser une table (11) des transitions permises.

19. Procédé selon la revendication 18, lorsque celle-ci dépend des revendications 13 à 17, caractérisé en ce que l'étape (53) d'exécution d'actions systématiques consiste :

- à exploiter une entrée (400, 401), correspondant à la transition demandée, d'une table (13) d'actions et ;
- à exécuter un programme d'actions (404) défini par ladite entrée.

20. Procédé selon l'une quelconque des revendications 18 ou 19, lorsque la revendication 18 dépend des revendications 14 à 16, caractérisé en ce que l'étape (52) d'évaluation des vérifications associées à la transition demandée, consiste :

- à exploiter une entrée (30) d'une table (12) des vérifications et ;
- à exécuter un programme (32) de vérifications défini par ladite entrée.

21. Procédé selon l'une quelconque des revendications 18 à 20, lorsque la revendication 18 dépend des revendications 15 à 16, caractérisé en ce que l'étape (56) d'exécution d'actions positives consiste, si la transition demandée est autorisée (51) et si les vérifications associées à la transition demandée sont satisfaites (54) :

- à exploiter une entrée (400, 402), correspondant à la transition demandée, d'une table (13) d'actions et ;
- à exécuter un programme (405) d'actions défini par ladite entrée.

22. Procédé selon l'une quelconque des revendications 18 à 21, lorsque la revendication 18 dépend de la revendication 16, caractérisé en ce que l'étape (55) d'exécution d'actions négatives consiste, si les vérifications associées à la transition demandée ne sont pas satisfaites (54) :

- à exploiter une entrée (400, 403), correspondant à la transition demandée, de la table (13) d'actions et ;
- à exécuter un programme (406) d'actions défini par ladite entrée.

23. Procédé selon l'une quelconque des revendications 18 à 19, lorsque la revendication 18 dépend de la revendication 17, caractérisé en ce que l'étape (56) d'exécution d'actions positives consiste, si la transition demandée est autorisée (51) :

- à exploiter une entrée (400, 402), correspondant à la transition demandée, d'une table (13) d'actions et ;
- à exécuter un programme (405) d'actions défini par ladite entrée.

24. Procédé selon l'une quelconque des revendications 12 à 17, mis en œuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état additif vers un second état additif, caractérisé en que l'étape (511) de validation de l'autorisation de ladite demande consiste à analyser une extension (16) d'une table (11) des transitions permises.

25. Procédé selon la revendication 24, lorsque celle-ci dépend des revendications 13 à 17, caractérisé en ce que l'étape (513) d'exécution d'actions systématiques consiste :

- à exploiter une entrée (407, 408), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;

- à exécuter un programme d'actions (411) défini par ladite entrée.

26. Procédé selon l'une quelconque des revendications 24 ou 25, lorsque la revendication 24 dépend des revendications 14 à 16, caractérisé en ce que l'étape (512) d'évaluation des vérifications associées à la transition demandée consiste :

- à exploiter une entrée (33) d'une extension (17) d'une table (12) des vérifications et ;
- à exécuter un programme (35) de vérifications défini par ladite entrée.

27. Procédé selon l'une quelconque des revendications 24 à 26, lorsque la revendication 24 dépend des revendications 15 à 16, caractérisé en ce que l'étape (516) d'exécution d'actions positives consiste, si la transition demandée est autorisée (511) et si les vérifications associées à la transition demandée sont satisfaites (514) :

- à exploiter une entrée (407, 409), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (412) défini par ladite entrée.

28. Procédé selon l'une quelconque des revendications 24 à 27, lorsque la revendication 24 dépend de la revendication 16, caractérisé en ce que l'étape (515) d'exécution d'actions négatives consiste, si les vérifications associées à la transition demandée ne sont pas satisfaites (514) :

- à exploiter une entrée (407, 410), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (413) défini par ladite entrée.

29. Procédé selon l'une quelconque des revendications 24 à 25, lorsque la revendication 24 dépend de la revendication 17, caractérisé en ce que l'étape (516) d'exécution d'actions positives consiste, si la transition demandée est autorisée (511) :

- à exploiter une entrée (407, 409), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (412) défini par ladite entrée.

30. Procédé selon l'une quelconque des revendications 12 à 17, mis en œuvre au sein de l'objet, à la suite d'une demande de transition d'un état de référence vers un état additif, caractérisé en que l'étape (528, 521) de validation de l'autorisation de ladite demande consiste à :

- valider (528) l'autorisation d'une transition dudit état de référence vers un état additif en analysant une table (11) des transitions permises;
- valider (521) l'autorisation d'une transition dudit état de référence vers ledit état additif en analysant une extension (16) de la table (11) des transitions permises.

31. Procédé selon la revendication 30, lorsque celle-ci dépend des revendications 13 à 17, caractérisé en ce que l'étape (513) d'exécution d'actions systématiques consiste :

- à exploiter une entrée (407, 408), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (411) défini par ladite entrée.

32. Procédé selon l'une quelconque des revendications 30 ou 31, lorsque la revendication 30 dépend des revendications

14 à 16, caractérisé en ce que l'étape (522) d'évaluation des vérifications associées à la transition demandée consiste :

- à exploiter une entrée (33) d'une extension (17) d'une table (12) des vérifications et ;
- à exécuter un programme (35) de vérifications défini par ladite entrée.

33. Procédé selon l'une quelconque des revendications 30 à 32, lorsque la revendication 30 dépend des revendications 15 à 16, caractérisé en ce que l'étape (526) d'exécution d'actions positives consiste, si la transition demandée est autorisée (528, 521) et si les vérifications associées à la transition demandée sont satisfaites (524) :

- à exploiter une entrée (407, 409), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (412) défini par ladite entrée.

34. Procédé selon l'une quelconque des revendications 30 à 33, lorsque la revendication 30 dépend de la revendication 16, caractérisé en ce que l'étape (525) d'exécution d'actions négatives consiste, si les vérifications associées à la transition demandée ne sont pas satisfaites (524) :

- à exploiter une entrée (407, 410), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;
- à exécuter un programme d'actions (413) défini par ladite entrée.

35. Procédé selon l'une quelconque des revendications 30 à 31, lorsque la revendication 30 dépend de la revendication 17, caractérisé en ce que l'étape (526) d'exécution d'actions positives consiste si la transition demandée est autorisée (528, 521) :

- à exploiter une entrée (407, 409), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions et ;

- à exécuter un programme d'actions (412) défini par ladite entrée.

36. Procédé selon l'une quelconque des revendications 12 à 35, caractérisé en ce que ledit procédé n'autorise pas le franchissement d'une transition d'état, d'un état additif vers un état de référence.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 555	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 02678	Date du dépôt international *(jour/mois/année)* 03/11/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 13/11/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé,**

   [ ] le texte est approuvé tel qu'il a été remis par le déposant

   [X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 1

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la pr mière feuille)

L'abrégé doit être modifié comme suit:

ligne 3: après 'puce' insérez '(1)';
ligne 6: après 'traitement' insérez '(2)';
ligne 6: après 'programmes' insérez '(4)';
ligne 7: après 'données' insérez '(5)';
ligne 9: après 'contrôle' insérez '(9, 11, 12).

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/02678

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/073 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 473 690 A (GRIMONPREZ GEORGES ET AL) 5 décembre 1995 (1995-12-05) le document en entier	1-27
A	WO 98 09257 A (GEMPLUS CARD INT) 5 mars 1998 (1998-03-05) page 14, ligne 4 -page 20, ligne 19	1,11
A	EP 0 583 006 A (MATSUSHITA ELECTRIC IND CO LTD) 16 février 1994 (1994-02-16) colonne 3, ligne 35 -colonne 7, ligne 5	1,11

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 janvier 2000	25/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Goossens, A

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 99/02678

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5473690 A	05-12-1995	FR 2673476 A	04-09-1992
		DE 69205425 D	16-11-1995
		DE 69205425 T	21-03-1996
		EP 0589884 A	06-04-1994
		ES 2082451 T	16-03-1996
		WO 9213322 A	06-08-1992
		JP 6504862 T	02-06-1994
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AU 4842897 A	19-03-1998
		CA 2233217 A	05-03-1998
		EP 0858644 A	19-08-1998
EP 0583006 A	16-02-1994	JP 2502894 B	29-05-1996
		JP 6060235 A	04-03-1994
		JP 6131517 A	13-05-1994
		DE 69320900 D	15-10-1998
		DE 69320900 T	28-01-1999
		KR 9706648 B	29-04-1997
		US 5408082 A	18-04-1995